Pro C7100s/C7100sx/C7110s/C7110sx

Instruções de operação

Guia de segurança

Para um uso seguro e correto, certifique-se de ler as Informações de segurança em 'Leia isto primeiro' antes de usar o equipamento.

CONTEÚDO

1. Instruções iniciais

2. Configurar a autenticação dos usuários

3. Restringir o uso do equipamento

4. Evitar vazamento de informações do equipamento

5. Segurança de rede avançada

6. Evitar vazamentos de documentos

7. Gerenciar o equipamento

8. Solução de problemas

9. Lista de privilégios de operações em definições

1. Instruções iniciais

Este capítulo descreve as precauções que você deve tomar ao usar os recursos de segurança da impressora e como configurar as definições de administrador.

Antes de configurar as definições de funções de segurança

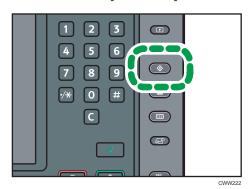
- **Se as definições de segurança não estiverem configuradas, os dados no equipamento estarão vulneráveis a ataques.**
- Para impedir que a impressora seja roubada ou danificada intencionalmente, instale-a em um local seguro.
- Os proprietários deste equipamento devem assegurar uma utilização adequada por parte dos usuários, de acordo com as operações determinadas pelo administrador e supervisor do equipamento. Se o administrador ou supervisor não efetuar as definições de segurança necessárias, existe o risco de falhas de segurança por parte dos usuários.
- Antes de definir os recursos de segurança do equipamento e para garantir utilização adequada por parte dos usuários, os administradores devem ler atentamente todo o Guia de segurança, prestando atenção especial ao capítulo "Antes de configurar as definições de funções de segurança".
- Os administradores devem informar os usuários sobre a utilização correta das funções de segurança.
- Se este equipamento estiver conectado a uma rede, o seu ambiente precisa estar protegido por um firewall ou uma ferramenta semelhante.
- Para proteção de dados durante a fase de comunicação, aplique as funções de segurança de comunicação do equipamento e conecte-o a dispositivos que suportem funções como comunicação criptografada.
- Os administradores devem examinar regularmente os registros do equipamento para verificar se existem eventos anormais.

Antes de usar o equipamento

Esta seção explica como ativar a criptografia de dados transmitidos e configurar a conta do administrador. Se você deseja um nível elevado de segurança, efetue a seguinte definição antes de utilizar o equipamento.

1. **Ligue o equipamento.**

   Para mais informações sobre como ligar a alimentação principal, consulte Getting Started.

2. **Pressione a tecla [User Tools].**

3. **Pressione [Definições do sistema].**
4. **Pressione [Definições de interface].**
5. **Especifique o endereço IPv4.**

   Para detalhes sobre como especificar o endereço IPv4, consulte Conexão da máquina/Definições do sistema.

6. **Pressione [Transf de arquivos] em [Definições do sistema].**
7. **Pressione [Endereço de e-mail do administrador] e, em seguida, especifique o endereço de e-mail do administrador deste equipamento.**
8. **Crie e instale o certificado do dispositivo a partir do painel de controle.**

   Para informações sobre como instalar o certificado do dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo".

   Como o endereço de e-mail para o certificado do dispositivo, insira o endereço especificado na Etapa 7.

9. **Altere o nome de usuário e a senha de login do administrador.**

   Para obter detalhes sobre a especificação de nomes de usuário e senhas de login dos administradores, consulte Pág. 17 "Registro e alteração de administradores".

10. **Conecte a máquina ao ambiente de rede de uso geral.**

- Para habilitar um nível mais alto de segurança, consulte Pág. 260 "Informações Adicionais para Segurança Avançada".

Administradores e usuários

Esta seção explica os termos "administrador", "supervisor", "usuário" e "proprietário", usados neste manual.

Administrador

Há quatro tipos de administradores para a máquina: administrador de usuário, administrador de equipamento, administrador de rede e administrador de arquivo.

Sua principal função é especificar as configurações para operar a máquina. Seus privilégios de acesso dependem do tipo de administrador. Os administradores não podem executar operações habituais como copiar e imprimir.

Supervisor

Há somente um supervisor.
O supervisor pode definir a senha de cada administrador.
Para operações habituais, não é necessário um supervisor, pois os próprios administradores definem suas senhas.

Usuário

Os usuários são aqueles que utilizam o equipamento para operações habituais, como copiar e imprimir.

Proprietário

O usuário que possui arquivos registrados no equipamento na função de copiadora, impressora ou em outras funções é chamado de proprietário.

Administradores

Os administradores gerenciam o acesso do usuário ao equipamento e várias outras funções e definições importantes.

Caso um administrador controle o acesso limitado e as definições, selecione primeiro o administrador do equipamento e ative a função de autenticação antes de utilizar o equipamento. Quando a função de autenticação está ativada, são necessários o nome de usuário e a senha de login para utilizar o equipamento. A função de administrador deste equipamento é dividida em quatro categorias, de acordo com sua função: administrador de usuários, administrador de equipamentos, administrador de redes e administrador de arquivos. O compartilhamento de tarefas facilita a tarefa de cada administrador e, ao mesmo tempo, evita operações não autorizadas do administrador. Um administrador pode ser designado para várias funções de administrador, sendo que uma função pode ser compartilhada por mais de um administrador. Também é possível criar um supervisor, que poderá alterar senhas de administradores.

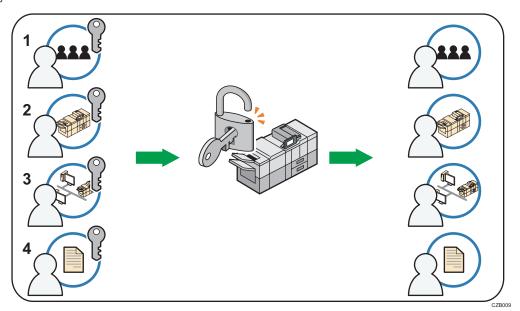
Os administradores não podem utilizar funções como cópia e impressão. Para utilizar estas funções, o administrador deve ser autenticado como usuário.

Para instruções sobre registro do administrador, consulte Pág. 17 "Registro e alteração de administradores", e sobre a alteração da senha do administrador, consulte Pág. 24 "Supervisor".
Para detalhes sobre usuários, consulte Pág. 27 "Usuários".

Configurar a autenticação de administrador

A autenticação de administrador requer o nome de usuário e a senha de login para verificação dos administradores que tentam especificar as definições do equipamento ou acessá-las em uma rede. Ao registrar um administrador, você não pode usar um nome de usuário já registrado no Catálogo de endereços. Os administradores são gerenciados de forma diferente dos usuários registrados no Catálogo de endereços. A autenticação do Windows e a autenticação LDAP não são realizadas por um administrador; por isso, um administrador pode fazer login mesmo que o servidor não esteja acessível devido a um problema de rede. Cada administrador é identificado através de um nome de usuário de login. Uma pessoa pode acumular mais de um tipo de função de administrador se forem atribuídos vários privilégios de administrador a um único nome de usuário de login. Para obter instruções sobre como registrar o administrador, consulte Pág. 17 "Registro e alteração de administradores".

Você pode especificar um nome de usuário, uma senha de login e uma senha de criptografia para cada administrador. A senha de criptografia é utilizada para criptografar dados transmitidos através de SNMPv3. Também é utilizada por aplicativos como Device Manager NX que utilizam SNMPv3. Os administradores estão limitados ao gerenciamento das definições do equipamento e ao controle do acesso dos usuários; portanto, não podem utilizar funções como cópia e impressão. Para utilizar essas funções, o administrador deve se registrar como usuário no Catálogo de endereços e, em seguida, ser autenticado. Especifique a autenticação de administrador e, em seguida, a autenticação de usuário. Para informações sobre como especificar a autenticação, consulte Pág. 29 "Configurar a Autenticação de Usuário".

Funções de cada administrador

1. **Administrador de usuário**

   Gerencia as informações pessoais no Catálogo de endereços.

   Um administrador de usuários pode registrar/excluir usuários no Catálogo de endereços ou alterar informações pessoais dos usuários.

   Os usuários registrados no Catálogo de endereços também podem alterar e excluir suas próprias informações pessoais.

   Se um usuário esquecer a senha, o administrador de usuários pode excluir essa senha e criar uma nova, permitindo ao usuário acessar novamente o equipamento.

2. **Administrador de equipamento**

   Principalmente gerencia a definição padrão. Você pode configurar o equipamento para que as definições padrão de cada função só possam ser especificadas pelo administrador de equipamentos. Ao efetuar essa configuração, você evita que usuários não autorizados alterem as definições e permite que o equipamento seja utilizado com segurança pelos seus usuários.

3. **Administrador de redes**

   Gerencia as definições de rede. Você pode definir o equipamento para que as definições da rede, como endereço IP e configurações de envio e recepção de e-mail, só possam ser especificadas pelo administrador de redes.

   Ao efetuar essa definição, você pode evitar que pessoas não autorizadas alterem as definições e desativem o equipamento, garantindo assim o correto funcionamento da rede.

4. **Administrador de arquivos**

   Gerencia a permissão para acessar os arquivos armazenados. Você pode especificar senhas para determinar que apenas usuários registrados tenham permissão para visualizar e editar arquivos armazenados no Servidor de documentos. Com essa definição, você evita o vazamento e a adulteração de dados decorrentes da exibição e do uso por usuários não autorizados dos dados registrados.

- A autenticação de administradores também pode ser especificada através do Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- Você pode especificar a autenticação por código de usuário sem especificar a autenticação de administrador.

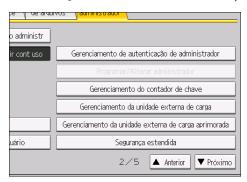
Especificar privilégios de administrador

Para especificar a autenticação de administrador, defina Gerenciamento de autenticação de administrador como [Ligado]. Se esta definição está ativada, os administradores podem configurar somente as definições alocadas para eles.

Para fazer login como administrador, utilize o nome de usuário e a senha de login padrão.

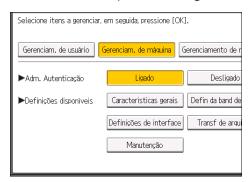
Para detalhes sobre como fazer login e logout com autenticação de administrador, consulte Pág. 21 "Método de login do administrador" e Pág. 23 "Método de logout de administrador".

- Se você tiver ativado o "Gerenciamento de autenticação de administrador", tenha cuidado para não esquecer o nome de usuário e a senha de login do administrador. Se você esquecer o nome do usuário ou a senha de login, deverá especificar uma nova senha usando os privilégios de supervisor. Para obter informações sobre os privilégios de supervisor, consulte Pág. 24 "Supervisor".

1. **Pressione a tecla [User Tools].**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Gerenciamento de autenticação de administrador].**

6. **Pressione [Gerenciam. de usuário], [Gerenciam. de máquina], [Gerenciamento de rede] ou [Gerenciam. de arquivos] para selecionar as definições a serem gerenciadas.**

7. **Defina "Adm. Autenticação" como [Ligado].**

   A opção "Definições disponíveis" é exibida.

8. **Selecione as definições a serem gerenciadas em "Definições disponíveis".**

As definições selecionadas não estarão disponíveis para os usuários.

As definições disponíveis dependem do tipo de administrador.

Para especificar a autenticação de administrador para mais de uma categoria, repita as etapas 6 a 8.

9. **Pressione [OK].**
10. **Pressione a tecla [User Tools].**

Registro e alteração de administradores

Se a autenticação de administrador é especificada, recomendamos que apenas uma pessoa assuma cada função de administrador.

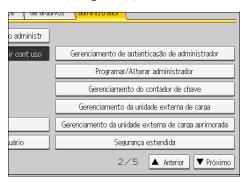
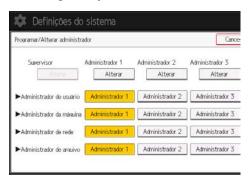
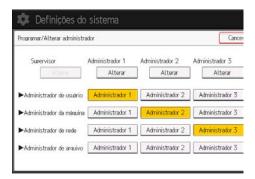
O compartilhamento de tarefas facilita a tarefa de cada administrador e, ao mesmo tempo, evita operações não autorizadas do administrador. Você pode registrar até 4 nomes de login (Administradores 1-4) aos quais pode conceder privilégios de administrador.

Os privilégios de um administrador só podem ser alterados por um administrador que tenha os privilégios relevantes.

Certifique-se de atribuir todos os privilégios de administrador para que cada privilégio de administrador fique associado a pelo menos um administrador.

Para detalhes sobre como fazer login e logout com autenticação de administrador, consulte Pág. 21 "Método de login do administrador" e Pág. 23 "Método de logout de administrador".

1. **Faça login como administrador no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**

5. **Pressione [Programar/Alterar administrador].**

6. **Na linha correspondente ao administrador cujos privilégios você deseja especificar, pressione [Administrador 1], [Administrador 2], [Administrador 3] ou [Administrador 4] e, em seguida, pressione [Alterar].**

Ao alocar privilégios de administrador para uma pessoa, selecione o administrador em cada categoria, conforma mostrado a seguir.

Para combinar diversos privilégios de administrador, atribua diversos privilégios de administrador a um único administrador.

Por exemplo, para atribuir privilégios de administrador do equipamento e privilégios de administrador de usuários ao [Administrador 1], pressione [Administrador 1] nas linhas referentes ao administrador do equipamento e ao administrador de usuários.

7. **Pressione [Alterar] para "Nome de usuário de login".**

8. **Insira o nome de usuário de login e pressione [OK].**
9. **Pressione [Alterar] para "Senha de login".**
10. **Insira a senha de login e pressione [OK].**

    Siga a política de senhas para reforçar a senha de login.

    Para informações sobre a política de senhas e como especificá-la, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".
11. **Insira a senha de login para confirmação novamente e pressione [OK].**
12. **Pressione [Alterar] para "Senha de criptografia".**
13. **Insira a senha de criptografia e, em seguida, pressione [OK].**
14. **Insira a senha de criptografia para confirmação novamente e pressione [OK].**
15. **Pressione [OK] duas vezes.**

    O logout será feito automaticamente.

- Para saber que caracteres podem ser usados para nomes de usuários e senhas de login, consulte Pág. 19 "Caracteres que podem ser usados para nomes de usuários e senhas".

Caracteres que podem ser usados para nomes de usuários e senhas

Os seguintes caracteres podem ser utilizados para nomes de usuários e senhas de login. Para nomes de usuários e senhas, há distinção entre letras maiúsculas e minúsculas.

- Maiúsculas: A a Z (26 caracteres)
- Minúsculas: a a z (26 caracteres)
- Números: 0 a 9 (10 caracteres)
- Símbolos: (espaço) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ (33 caracteres)

Nome de usuário de login

- Não pode conter espaços, ponto e vírgula ou aspas.
- Não pode ser deixado em branco.
- É possível usar até 32 caracteres.
- O nome do usuário do login de um administrador deve conter caracteres diferentes de caracteres numéricos (números) se tiver até oito caracteres. Se consistir apenas de números, nove ou mais devem ser usados.

Senha de login

- O tamanho máximo da senha dos administradores e supervisores é de 32 caracteres; para usuários é de 128 caracteres.

- Não há restrições para tipos de caracteres que podem ser usados para uma senha. Por segurança, recomenda-se criar senhas consistindo de caracteres maiúsculos e minúsculos, números e símbolos. Uma senha consistindo de um grande número de caracteres é menos provável de ser adivinhada.
- Em [Política de Senha] em [Segurança estendida], você pode especificar uma senha consistindo de caracteres maiúsculos e minúsculos, números e símbolos, assim como o número mínimo de caracteres a serem usados para a senha. Para obter detalhes sobre a política de especificação de senha, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

Utilizar o Web Image Monitor para configurar a autenticação de administrador

Utilizando o Web Image Monitor, você pode fazer login no equipamento e alterar as definições de administrador. Para detalhes sobre como fazer login e logout com autenticação de administrador, consulte Pág. 21 "Método de login do administrador" e Pág. 23 "Método de logout de administrador".

1. **Faça login no Web Image Monitor como administrador.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Gerenciamento de autenticação de administrador] ou [Programar/Alterar administrador] em "Definições do dispositivo".**
4. **Altere as definições, conforme desejado.**
5. **Faça logout.**

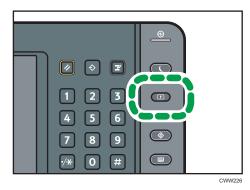
- Para mais informações sobre o Web Image Monitor, consulte a Ajuda do Web Image Monitor.

Método de login do administrador

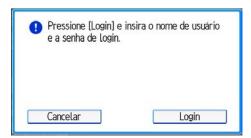
Se a autenticação de administrador for especificada, faça login usando um nome e uma senha de login de administrador. O login de supervisores é feito da mesma maneira.

Para obter informações sobre o nome de usuário e a senha de administrador e supervisor, consulte o administrador.

Fazer login utilizando o painel de controle

1. **Pressione a tecla [User Tools].**
2. **Pressione a tecla [Login/Logout].**

A tela de login aparece.

A tela de login também pode aparecer pressionando [Login] no menu Ferramentas do usuário.

3. **Pressione [Login].**

4. **Insira o nome de usuário de login e pressione [OK].**
5. **Insira a senha de login e pressione [OK].**

"Autenticando... Aguarde. " aparece, seguido da tela de definições iniciais.

- Se a autenticação de usuário já tiver sido especificada, aparecerá uma tela para autenticação. Para fazer login como administrador, insira o nome de usuário e a senha de login.

- Se você fizer login usando privilégios de administrador, será mostrado o nome do administrador que está fazendo login. Quando você fizer login com um nome de usuário com vários privilégios de administrador, um dos privilégios de administrador associado ao nome é exibido.
- Se você tentar fazer login em uma tela de operação, "Você não tem os privilégios necessários para usar essa função. Só é possível alterar a(s) definição(ões) como administrador." será exibido. Pressione a tecla [User Tools] para exibir a tela de definições iniciais.

Fazer login utilizando o Web Image Monitor

1. **Abra um navegador da Web.**
2. **Insira "http://(endereço IP o nome do host da impressora)/" na barra de endereços.**

   Ao inserir um endereço IPv4, não comece os segmentos com zeros. Por exemplo, se o endereço for "192.168.001.010", você deve inseri-lo como "192.168.1.10" para conectar o equipamento.

   Insira o endereço IPv6 entre colchetes, como, por exemplo: [2001:db8::9abc].

   Se você definir "Permitir comunicação SSL/TLS" como [Somente texto cifrado], insira " https://(IP do equipamento ou nome do host)/" para acessar o equipamento.
3. **Clique em [Login] no canto superior direito da janela.**
4. **Insira o nome de usuário e a senha de login de um administrador e, em seguida, clique em [Login].**

- O navegador pode estar configurado para preencher automaticamente as caixas de diálogo de login mantendo os nomes de usuário e senhas de login. Essa função diminui a segurança. Para evitar que o navegador mantenha os nomes de usuário e as senhas de login, desative a função de preenchimento automático do navegador.

Método de logout de administrador

Se a autenticação do administrador é especificada, não esqueça de fazer o logout após efetuar as mudanças nas definições. O logout de supervisores é feito da mesma maneira.

Fazer logout usando o painel de controle

1. **Pressione a tecla [Login/Logout] e, em seguida, pressione [Sim].**

- Você também pode fazer logout utilizando os procedimentos a seguir:
  - Pressione a tecla [Economia de energia].

Fazer logout utilizando o Web Image Monitor

1. **Clique em [Logout] no canto superior direito da janela.**

- Depois de fazer logout, exclua a memória cache no Web Image Monitor.

Supervisor

O supervisor pode excluir a senha de um administrador e especificar uma nova.

Se um administrador esquece ou muda sua senha, o supervisor pode atribuir uma nova senha para o administrador. Se você fez login utilizando o nome de usuário e a senha do supervisor, não poderá usar as funções normais ou fazer definições do sistema. Os métodos de login e logout são os mesmos dos administradores. Consulte Pág. 21 "Método de login do administrador" e Pág. 23 "Método de logout de administrador".

Importante

- **Tenha cuidado para não esquecer o nome de usuário e a senha de login de supervisor. Caso se esqueça, a assistência técnica precisará restaurar o equipamento para o estado padrão. Essa ação causará perda dos dados de definições, contadores, logs e outros dados do equipamento. A chamada de manutenção talvez seja cobrada.**

- Para saber que caracteres podem ser usados para nomes de usuários e senhas de login, consulte Pág. 19 "Caracteres que podem ser usados para nomes de usuários e senhas".
- Você não pode especificar o mesmo nome de usuário de login para o supervisor e para os administradores.
- Utilizando o Web Image Monitor, você pode fazer login como supervisor e excluir a senha de um administrador ou especificar uma nova.

Redefinir a senha do administrador

1. **Faça login como supervisor no painel de controle.**

   Para obter informações sobre como fazer login, consulte Pág. 21 "Método de login do administrador".
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Programar/Alterar administrador].**

6. **Pressione [Alterar] do administrador que deseja redefinir.**

7. **Pressione [Alterar] para "Senha de login".**
8. **Insira a senha de login e pressione [OK].**
9. **Insira a senha de login para confirmação novamente e pressione [OK].**
10. **Pressione [OK] duas vezes.**

    O logout será feito automaticamente.

- O supervisor pode alterar as senhas de login dos administradores, mas não seus nomes de usuário de login.

Alterar o supervisor

Esta seção descreve como alterar o nome de usuário e senha de login do supervisor.

Para isso, é necessário ativar os privilégios de administrador do usuário através das definições em "Gerenciamento de autenticação de administrador". Para mais informações, consulte Pág. 15 "Especificar privilégios de administrador".

1. **Faça login como supervisor no painel de controle.**

   Para obter informações sobre como fazer login, consulte Pág. 21 "Método de login do administrador".
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Programar/Alterar administrador].**
6. **Em "Supervisor", pressione [Alterar].**
7. **Pressione [Alterar] para "Nome de usuário de login".**
8. **Insira o nome de usuário de login e pressione [OK].**
9. **Pressione [Alterar] para "Senha de login".**

10. Insira a senha de login e pressione [OK].

11. Insira a senha de login para confirmação novamente e pressione [OK].

12. Pressione [OK] duas vezes.

O logout será feito automaticamente.

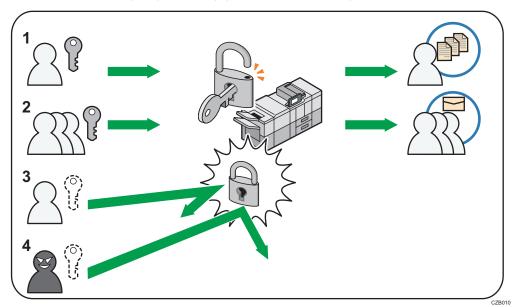
2. Configurar a autenticação dos usuários

Este capítulo descreve como especificar a autenticação de usuário e explica as funções que são ativadas pela autenticação de usuário.

Usuários

Um usuário executa operações normais no equipamento, como cópia e impressão. Os usuários são gerenciados por meio das informações no Catálogo de endereços do equipamento e só podem utilizar as funções às quais têm acesso concedido pelos administradores. Ativando a autenticação de usuário, você pode permitir que apenas pessoas registradas no Catálogo de endereços utilizem o equipamento. Os usuários podem ser gerenciados no Catálogo de endereços pelo administrador de usuários. Para obter mais informações sobre administradores, consulte Pág. 13 "Administradores". Para obter mais informações sobre registro no Catálogo de endereços, consulte Connecting the Machine/ System Settings ou a Ajuda do Web Image Monitor.

Sobre a autenticação de usuário

A autenticação do usuário é um sistema que requer o nome de usuário e a senha de login para verificação de usuários que operam o equipamento ou o acessam pela rede.

1. **Usuário**

   Um usuário executa operações normais no equipamento, como cópia e impressão.

2. **Grupo**

   Um grupo executa operações normais no equipamento, como cópia e impressão.

3. **Usuário não autorizado**

4. **Acesso não autorizado**

Configurar a Autenticação de Usuário

Existem quatro tipos de métodos de autenticação de usuário: autenticação por código de usuário, autenticação básica, autenticação do Windows e autenticação LDAP. Para usar a autenticação de usuário, selecione um método de autenticação no painel de controle e, em seguida, efetue as definições necessárias para a autenticação. As definições dependem do método de autenticação. Especifique a autenticação de administrador e, em seguida, a autenticação de usuário.

Importante

- **Se a autenticação de usuário não puder ser ativada devido a um problema com o disco rígido ou com a rede, você pode utilizar o equipamento efetuando o acesso através da autenticação de administrador e desativando a autenticação de usuário. Proceda dessa forma se, por exemplo, precisar utilizar o equipamento com urgência.**
- **Você não pode utilizar mais de um método de autenticação ao mesmo tempo.**

Fluxo de configuração da autenticação de usuário

Procedimento de configuração	Detalhes
Configuração da autenticação de administrador	Pág. 15 "Especificar privilégios de administrador" Pág. 17 "Registro e alteração de administradores"
Configuração da autenticação de usuário	Especifique a autenticação de usuário. Estão disponíveis 4 tipos de autenticação de usuário: • Pág. 32 "Autenticação por código de usuário" • Pág. 34 "Autenticação básica" • Pág. 39 "Autenticação do Windows" • Pág. 48 "Autenticação LDAP"

Métodos de autenticação de usuário

Tipo	Detalhes
Autenticação de código de usuário	A autenticação é realizada utilizando códigos de usuário de oito dígitos. A autenticação é aplicada a cada código de usuário e não a cada usuário. É necessário registrar o código de usuário no Catálogo de endereços do equipamento com antecedência.

Tipo	Detalhes
Autenticação básica	A autenticação é realizada utilizando o Catálogo de endereços do equipamento. É necessário registrar os usuários no Catálogo de endereços com antecedência. A autenticação pode ser aplicada a cada usuário.
Autenticação do Windows	A autenticação é realizada utilizando o controlador de domínio do servidor do Windows na mesma rede do equipamento. A autenticação pode ser aplicada a cada usuário.
Autenticação LDAP	A autenticação é realizada utilizando o servidor LDAP na mesma rede do equipamento. A autenticação pode ser aplicada a cada usuário.

O endereço de e-mail de um usuário obtido por meio de autenticação Windows ou LDAP pode ser usado como o endereço fixo do remetente ("De") quando você envia e-mails no modo de scanner para evitar fraude de ID.

Se o método de autenticação de usuário for trocado durante o processo

- É possível transferir e utilizar como nome de usuário de login uma conta de código de usuário que não tenha mais de oito dígitos e que seja utilizada para autenticação por código de usuário, mesmo depois de o método de autenticação mudar de autenticação por código de usuário para autenticação básica, autenticação do Windows ou autenticação LDAP. Nesse caso, uma vez que a autenticação de Código de usuário não tem uma senha, a senha de login fica em branco.
- Se o método de autenticação mudar para método de autenticação externa (autenticação do Windows ou autenticação LDAP), a autenticação não poderá ser efetuada, a não ser que a conta de código de usuário transferida tenha sido previamente registrada no dispositivo externo. No entanto, a conta de código de usuário será armazenada no Catálogo de endereços mesmo quando há falha na autenticação.
- Do ponto de vista da segurança, ao mudar a autenticação por Código de usuário para outro método de autenticação, recomenda-se excluir contas não utilizadas ou configurar uma senha de login. Para mais detalhes sobre como excluir contas, consulte Conexão da máquina/Definições do sistema. Para informações sobre como alterar senhas, consulte Pág. 36 "Especificar nomes de usuários e senhas".

- Depois de ligar o equipamento, os recursos estendidos podem não aparecer na lista de itens para autenticação do usuário no menu Gerenciamento de autenticação de usuário. Se isso acontecer,

aguarde alguns instantes e, em seguida, abra o menu Gerenciamento de autenticação de usuário novamente.

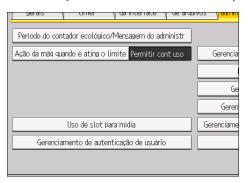
- A autenticação de usuário também pode ser especificada via Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Autenticação por código de usuário

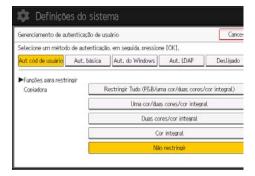
Esse é um método de autenticação para limitar o acesso a funções de acordo com um código de usuário. O mesmo código de usuário pode ser utilizado por diversos usuários.

Para obter mais informações sobre como especificar códigos de usuários, consulte Connecting the Machine/ System Settings.

Para obter informações sobre como especificar o código de usuário no driver da impressora ou driver TWAIN, consulte a Ajuda do driver.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Gerenciamento de autenticação de usuário].**

6. **Selecione [Aut cód de usuário].**

   Se não quiser ativar a autenticação de usuário, selecione [Desligado].

7. **Em "Funções para restringir", selecione as funções que deseja restringir.**

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

A funções selecionadas estão sujeitas à autenticação por código de usuário. A autenticação por código de usuário não é aplicada às funções não selecionadas.

Para informações sobre como limitar as funções disponíveis a pessoas ou grupos, consulte Pág. 70 "Limitar as Funções disponíveis".

8. **Para especificar uma autenticação de trabalho de impressora, selecione um item diferente de [Controle de PC] para "Impressora" em "Funções para restringir".**

   Se os itens não forem visualizados, pressione, [▼Próximo].

   Se não desejar especificar a autenticação de trabalho de impressora, vá para a etapa 14.

9. **Pressione [▼Próximo].**
10. **Selecione o nível de "Autenticação de trabalho de impressora".**

    Para obter uma descrição dos níveis de autenticação dos trabalhos da impressora, consulte Pág. 53 "Autenticação de trabalhos da impressora".

    Se você selecionar [Inteiro] ou [Simples (Tudo)], vá para a etapa 14.

    Se você selecionar [Simples (Limitação)], vá para a etapa 11.

11. **Pressione [Alterar] para "Intervalo de limitação".**
12. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autentic trab impressora".**

Você pode especificar o intervalo do endereço IPv4 ao qual será aplicada essa definição.

13. **Pressione [Sair].**
14. **Pressione [OK].**
15. **Pressione a tecla [Login/Logout].**

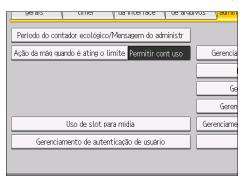
    Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Autenticação básica

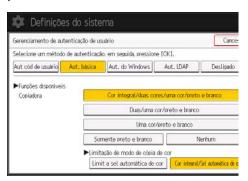
Especifique esse método de autenticação quando utilizar o Catálogo de endereços do equipamento para autenticar cada usuário. Utilizando a autenticação básica, você pode não apenas gerenciar as funções disponíveis do equipamento como também limitar o acesso a arquivos armazenados e ao Catálogo de endereços. Na autenticação básica, o administrador precisa especificar as funções disponíveis para cada usuário registrado no Catálogo de endereços. Para obter detalhes sobre como limitar as funções, consulte Pág. 36 "Informações de autenticação armazenadas no Catálogo de endereços".

Especificar a autenticação básica

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador esteja devidamente configurada em "Gerenciamento de autenticação de administrador".

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Gerenciamento de autenticação de usuário].**

6. **Selecione [Aut. básica].**

   Se não quiser ativar a autenticação de usuário, selecione [Desligado].

7. **Em "Funções disponíveis", selecione qual das funções do equipamento você deseja permitir.**

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

As funções que você selecionar aqui se tornam as definições padrão de autenticação básica que serão atribuídas a todos os novos usuários do Catálogo de endereços.

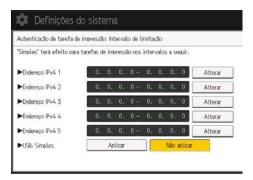
Para informações sobre como especificar as funções disponíveis a pessoas ou grupos, consulte Pág. 70 "Limitar as Funções disponíveis".

8. **Pressione [▼Próximo].**
9. **Selecione o nível de "Autenticação de trabalho de impressora".**

Para obter uma descrição dos níveis de autenticação dos trabalhos da impressora, consulte Pág. 53 "Autenticação de trabalhos da impressora".

Se você selecionar [Inteiro] ou [Simples (Tudo)], vá para a etapa 13.

Se você selecionar [Simples (Limitação)], vá para a etapa 10.

10. **Pressione [Alterar] para "Intervalo de limitação".**
11. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autentic trab impressora".**

Você pode especificar o intervalo do endereço IPv4 ao qual será aplicada essa definição.

12. **Pressione [Sair].**
13. **Pressione [OK].**

14. **Pressione a tecla [Login/Logout].**

    Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Informações de autenticação armazenadas no Catálogo de endereços

Se você ativou a autenticação de usuário, pode especificar os limites de acesso e de utilização para as funções do equipamento para cada usuário ou grupo de usuários. Especifique as definições necessárias na entrada de cada usuário do Catálogo de endereços. Para detalhes sobre as funções que podem ser limitadas, consulte Pág. 70 "Limitar as Funções disponíveis".

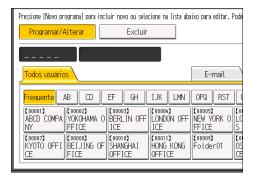
Os usuários devem ter uma conta registrada no Catálogo de endereços para utilizar o equipamento quando a autenticação de usuário é especificada. Para obter mais informações sobre o registro de usuários no Catálogo de endereços, consulte Connecting the Machine/ System Settings.

A autenticação de usuário também pode ser especificada via Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Especificar nomes de usuários e senhas

Em "Gerenciamento de Catálogo de endereços", especifique o nome de usuário e a senha de login a serem utilizados para o "Gerenciamento de autenticação de usuário".

Para saber que caracteres podem ser usados para nomes de usuários e senhas de login, consulte Pág. 19 "Caracteres que podem ser usados para nomes de usuários e senhas".

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário.**

4. **Pressione [Inform Aut.].**

5. **Pressione [Alterar] para "Nome de usuário de login".**
6. **Insira um nome de usuário de login e, em seguida, pressione [OK].**
7. **Pressione [Alterar] para "Senha de login".**
8. **Insira uma senha de login e, em seguida, pressione [OK].**
9. **Reinsira a senha de login para confirmação e pressione [OK].**
10. **Pressione [OK].**
11. **Pressione [Sair].**
12. **Faça logout.**

Especificar detalhes de login

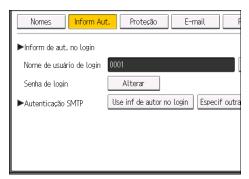
O nome de usuário e a senha de login especificados em "Gerenciamento de catálogo de endereços" podem ser utilizados como informações de login para "Autenticação SMTP", "Autenticação de pasta" e "Autenticação de LDAP".

Se você não deseja utilizar o nome de usuário e a senha de login especificados em "Gerenciamento de catálogo de endereços" para "Autenticação SMTP", "Autenticação de pasta" ou "Autenticação de LDPA", consulte Conexão da máquina/Definições do sistema.

Importante

- Ao utilizar "Use inf de autor no login" para "Autenticação SMTP", "Autenticação de pasta" ou "Autenticação de LDAP", um nome de usuário diferente de "other", "admin", "supervisor" ou "HIDE***" deve ser especificado. O símbolo "***" representa qualquer caractere.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário.**
4. **Pressione [Inform Aut.].**

5. **Selecione [Use inf de autor no login] em "Autenticação SMTP".**

Para autenticação da pasta, selecione [Use inf de autor no login] em "Autenticação de pasta".

Para autenticação LDAP, selecione [Use inf de autor no login] em "Autenticação de LDAP".

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

6. **Pressione [OK].**
7. **Pressione [Sair].**
8. **Faça logout.**

Autenticação do Windows

Especifique essa autenticação quando utilizar o controlador de domínio do Windows para autenticar os usuários que têm as suas contas no servidor de diretórios. Os usuários não podem ser autenticados se não tiverem conta no servidor de diretórios. Com a autenticação do Windows, você pode especificar o limite de acesso para cada grupo registrado no servidor de diretórios. O Catálogo de endereços armazenado no servidor de diretórios pode ser registrado no equipamento, permitindo a autenticação do usuário sem utilizar primeiro o equipamento para registrar as definições individuais no Catálogo de endereços.

Ao acessar o equipamento pela primeira vez, você pode utilizar as funções disponíveis para o seu grupo. Se você não estiver registrado em um grupo, poderá utilizar as funções disponíveis em "*Grupo padrão". Para limitar as funções disponíveis somente para certos usuários, primeiro faça as definições no Catálogo de endereços.

Para registrar automaticamente as informações do usuário na autenticação Windows, é aconselhável utilizar a criptografia SSL na comunicação entre o equipamento e a controladora de domínio. Para isso, você deve criar um certificado de servidor para o controlador de domínio. Para obter mais informações sobre como criar um certificado de servidor, consulte Pág. 47 "Criar o certificado de servidor".

Importante

- Se utilizar a autenticação Windows, as informações do usuário registradas no servidor de diretório são automaticamente registradas no Catálogo de endereços do equipamento. Mesmo que as informações do usuário automaticamente registradas no Catálogo de endereços do equipamento sejam editadas no equipamento, elas serão substituídas pelas informações do servidor de diretórios quando a autenticação for efetuada.
- Os usuários gerenciados em outros domínios estão sujeitos a autenticação do usuário, mas não podem obter itens como nomes de usuário.
- Se a autenticação Kerberos e a criptografia SSL forem definidas ao mesmo tempo, não será possível obter endereços de e-mail.
- Se foi criado um novo usuário no controlador de domínio e a opção "O usuário deve alterar a senha no próximo logon" foi selecionada durante a configuração de senha, faça logon no computador e altere a senha.
- Se o servidor de autenticação suportar apenas NTLM quando a autenticação Kerberos for selecionada no equipamento, o método de autenticação mudará automaticamente para NTLM.
- Quando a autenticação do Windows é usada, o nome de usuário de login diferencia maiúsculas e minúsculas. Um nome de usuário de login inserido incorretamente será adicionado ao Catálogo de endereços. Neste caso, exclua o usuário adicionado.
- Se a conta "Convidado" no servidor Windows estiver ativa, os usuários não registrados no controlador de domínio poderão ser autenticados. Quando essa conta é ativada, os usuários são

registrados no Catálogo de endereços e podem utilizar as funções disponíveis no "*Grupo padrão".

A autenticação do Windows pode ser executada utilizando um dos dois métodos de autenticação: autenticação NTLM ou Kerberos. Os requisitos operacionais para ambos os métodos estão listados abaixo:

Requisitos operacionais para a autenticação NTLM

Para especificar a autenticação NTLM, os seguintes requisitos devem ser atendidos:

- Este equipamento suporta as autenticações NTLMv1 e NTLMv2.
- Defina um controlador de domínio no domínio a ser utilizado.
- Esta função é suportada pelos sistemas operacionais listados abaixo. Para obter informações do usuário ao executar o Active Directory, utilize LDAP. Se utilizar LDAP, recomendamos que use SSL para criptografar a comunicação entre o equipamento e o servidor LDAP. A criptografia por SSL é possível apenas se o servidor LDAP suportar TLSv1 ou SSLv3.
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2
    - Windows Server 2012/2012 R2

Requisitos operacionais para a autenticação Kerberos

Para especificar a autenticação Kerberos, os seguintes requisitos devem ser atendidos:

- Defina um controlador de domínio no domínio a ser utilizado.
- O sistema operacional deve suportar KDC (Key Distribution Center). Para obter informações do usuário ao executar o Active Directory, utilize LDAP. Se utilizar LDAP, recomendamos que use SSL para criptografar a comunicação entre o equipamento e o servidor LDAP. A criptografia por SSL é possível apenas se o servidor LDAP suportar TLSv1 ou SSLv3. Os sistemas operacionais compatíveis estão listados abaixo:
    - Windows Server 2003/2003 R2
    - Windows Server 2008/2008 R2
    - Windows Server 2012/2012 R2

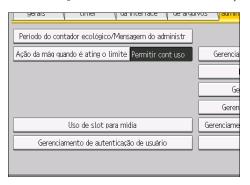
    Para utilizar a autenticação Kerberos no Windows Server 2008, instale o Service Pack 2 ou posterior.
- A transmissão de dados entre o equipamento e o servidor KDC será criptografada se a autenticação Kerberos estiver ativada. Para obter mais informações sobre como especificar uma transmissão criptografada, consulte Pág. 165 "Definições de criptografia da autenticação Kerberos".

- Para saber que caracteres podem ser usados para nomes de usuários e senhas de login, consulte Pág. 19 "Caracteres que podem ser usados para nomes de usuários e senhas".

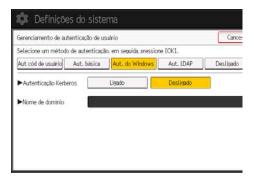
- Na próxima vez em que acessar o equipamento, será possível utilizar todas as funções disponíveis para o seu grupo e para você como usuário individual.
- Os usuários registrados em vários grupos podem utilizar todas as funções disponíveis para esses grupos.
- Com a autenticação do Windows, não é necessário criar um certificado de servidor, a menos que deseje registrar automaticamente as informações do usuário, como nomes de usuários utilizando SSL.

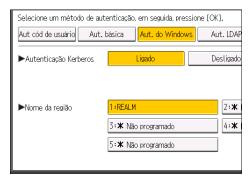
Especificar a autenticação do Windows

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador esteja devidamente configurada em "Gerenciamento de autenticação de administrador".

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Gerenciamento de autenticação de usuário].**

6. **Selecione [Aut. do Windows].**

   Se não quiser ativar a autenticação de usuário, selecione [Desligado].

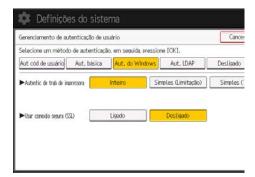
7. **Se quiser utilizar a autenticação Kerberos, pressione [Ligado].**

Se quiser utilizar a autenticação NTLM, pressione [Desligado] e avance para a etapa 9.

8. **Selecione o realm de autenticação Kerberos e avance para a etapa 10.**

Para ativar a autenticação Kerberos, é necessário registrar previamente um realm. Um nome do realm deve ser registrado em maiúsculas. Para obter mais informações sobre o registro de um realm, consulte Connecting the Machine/ System Settings.

É possível registrar até 5 realms.

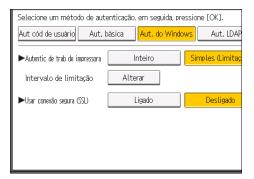
9. **Pressione [Alterar] para "Nome de domínio", insira o nome do controlador de domínio a ser autenticado e, em seguida, pressione [OK].**

10. **Pressione [▼Próximo].**

11. **Selecione o nível de "Autenticação de trabalho de impressora".**

Para obter uma descrição dos níveis de autenticação dos trabalhos da impressora, consulte Pág. 53 "Autenticação de trabalhos da impressora".

Se você selecionar [Inteiro] ou [Simples (Tudo)], vá para a etapa 15.

Se você selecionar [Simples (Limitação)], vá para a etapa 12.

12. Pressione [Alterar].

13. Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autentic trab impressora".

Você pode especificar o intervalo do endereço IPv4 ao qual será aplicada essa definição.

14. Pressione [Sair].

15. Pressione [Ligado] para "Usar conexão segura(SSL)".

Se não estiver usando Secure Sockets Layer (SSL) na autenticação, pressione [Desligado].

Se você não tiver registrado um grupo global, avance para a etapa 22.

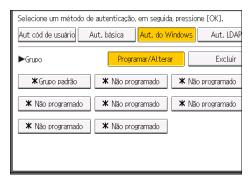
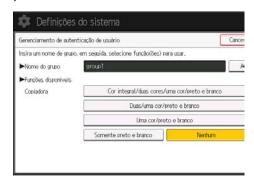
Se já tiver registrado um grupo global, avance para a etapa 16.

Se grupos globais foram registrados no servidor do Windows, você pode limitar a utilização de funções para cada grupo global.

É necessário criar antecipadamente grupos globais no servidor do Windows e registrar em cada grupo os usuários a serem autenticados. Também é necessário registrar no equipamento as funções disponíveis para os membros do grupo global. Crie grupos globais no equipamento inserindo os nomes dos grupos globais registrados no servidor do Windows. (Lembre-se de que,

nos nomes dos grupos, distinguem-se maiúsculas de minúsculas.) Em seguida, especifique as funções do equipamento disponíveis para cada grupo.

Se grupos globais não foram especificados, os usuários podem utilizar as funções especificadas em [*Grupo padrão]. Se estiverem especificados grupos globais, os usuários não registrados em grupos globais podem utilizar as funções disponíveis especificadas em [*Grupo padrão]. Por padrão, todas as funções estão disponíveis para membros do *Grupo padrão. Especifique a limitação das funções disponíveis de acordo com as necessidades dos usuários.

16. **Pressione [▼Próximo].**
17. **Em "Grupo", pressione [Programar/Alterar] e, em seguida, pressione [* Não programado].**

18. **Pressione [Alterar] para "Nome do grupo" e insira o nome do grupo.**
19. **Pressione [OK].**
20. **Em "Funções disponíveis", selecione qual das funções do equipamento você deseja permitir.**

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

A autenticação do Windows será aplicada às funções selecionadas.

Os usuários só podem utilizar as funções selecionadas.

Para informações sobre como especificar as funções disponíveis a pessoas ou grupos, consulte Pág. 70 "Limitar as Funções disponíveis".

21. **Pressione [OK].**

22. **Pressione [OK].**
23. **Pressione a tecla [Login/Logout].**

    Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Instalar o Internet Information Services (IIS) e Serviços de Certificados

Especifique essa definição se desejar que o equipamento obtenha automaticamente informações do usuário registradas no Active Directory.

Recomendamos que instale o Internet Information Services (IIS) e Serviços de Certificados como componentes do Windows.

Instale os componentes e crie o certificado de servidor.

Se não estiverem instalados, instale-os do seguinte modo:

Instalação com o Windows Server 2008 R2

1. **No menu [Iniciar], vá a [Ferramentas de administrador] e, em seguida, clique em [Gestor de servidores].**
2. **Clique em [Funções] na coluna esquerda e clique em [Adicionar Funções] no menu [Ação].**
3. **Clique em [Próximo>].**
4. **Marque as caixas de seleção "Servidor Web (IIS)" e "Serviços de Certificados do Active Directory" e, em seguida, clique em [Próximo>].**

    Se aparecer uma mensagem de confirmação, clique em [Adicionar Recursos].
5. **Leia as informações do conteúdo e, em seguida, clique em [Próximo>].**
6. **Verifique se a opção [Autoridade de Certificação] está marcada e clique em [Próximo>].**
7. **Selecione [Enterprise] e, em seguida, clique em [Próximo>].**
8. **Selecione [AC raiz] e, em seguida, clique em [Próximo>].**
9. **Selecione [Criar uma nova chave privada] e, em seguida, clique em [Próximo>].**
10. **Selecione um provedor de serviços de criptografia, o comprimento da chave e o algoritmo de hash para criar uma nova chave privada e, em seguida, clique em [Próximo>].**
11. **Em "Nome da autoridade de certificação:", insira o nome da autoridade de certificação e, em seguida, clique em [Próximo>].**
12. **Selecione o período de validade e, em seguida, clique em [Próximo>].**

13. Defina a "Localização do banco de dados de certificados:" e "Localização do log do banco de dados de certificados:" e, em seguida, clique em [Próximo>].
14. Leia as notas e, em seguida, clique em [Próximo>].
15. Selecione o serviço da função que deseja utilizar e, em seguida, clique em [Próximo>].
16. Clique em [Instalar].
17. Quando a instalação estiver concluída, clique em [Fechar].
18. Feche o [Gerenciador de Servidores].

Instalação com o Windows Server 2012

1. Na tela inicial, clique em [Gerenciador de Servidores].
2. No menu [Gerenciar], clique em [Adicionar Funções e Recursos].
3. Clique em [Próximo>].
4. Selecione [Instalação baseada em função ou recurso] e depois clique em [Próximo>].
5. Selecione um servidor e, em seguida, clique em [Próximo>].
6. Marque as caixas de seleção "Serviços de Certificados do Active Directory" e "Servidor Web (IIS)" e, em seguida, clique em [Próximo>].

   Se aparecer uma mensagem de confirmação, clique em [Adicionar Recursos].
7. Marque os recursos que deseja instalar e, em seguida, clique em [Próximo>].
8. Leia as informações do conteúdo e, em seguida, clique em [Próximo>].
9. Certifique-se que [Autoridade de Certificado] esteja selecionado na área [Serviços de Função] dos [Serviços de Certificados do Active Directory] e depois clique em [Próximo>].
10. Leia as informações do conteúdo e, em seguida, clique em [Próximo>].
11. Marque os serviços de função que deseja instalar em [Servidor Web (IIS)] e depois clique em [Próximo>].
12. Clique em [Instalar].
13. Após concluir a instalação, clique no ícone de notificação do gerenciador de servidores e clique em [Configurar os Serviços de Certificados do Active Directory no servidor de destino].
14. Clique em [Próximo>].
15. Clique em [Autoridade de Certificação] na área [Serviços de Função] e depois clique em [Próximo>].
16. Selecione [Empresa] e, em seguida, clique em [Próximo>].
17. Selecione [AC raiz] e, em seguida, clique em [Próximo>].
18. Selecione [Criar uma nova chave privada] e, em seguida, clique em [Próximo>].

19. **Selecione um provedor de criptografia, o tamanho da chave e o algoritmo de hash para criar uma nova chave privada e, em seguida, clique em [Próximo>].**
20. **Em "Nome da autoridade de certificação:", insira o nome da autoridade de certificação e, em seguida, clique em [Próximo>].**
21. **Selecione o período de validade e, em seguida, clique em [Próximo>].**
22. **Defina a "Localização do banco de dados de certificados:" e "Localização do log do banco de dados de certificados:" e, em seguida, clique em [Próximo>].**
23. **Clique em [Configurar].**
24. **Se aparecer a mensagem "Configuração bem-sucedida", clique em [Fechar].**

Criar o certificado de servidor

Depois de instalar os componentes do Windows Internet Information Services (IIS) e Serviços de Certificados, crie o certificado de servidor do seguinte modo:

O servidor Windows 2008 R2 é usado para exibir o procedimento.

1. **No menu [Iniciar], vá a [Ferramentas de administrador] e, em seguida, clique em [Gestor de Serviços de Informação Internet (IIS)].**

   No Windows Server 2012, clique em [Gerenciador do Serviços de Informações da Internet (IIS)] na tela inicial.

   Quando a mensagem de confirmação aparecer, clique em [Sim].
2. **Na coluna esquerda, clique no nome do servidor e, em seguida, clique duas vezes em [Certificados de Servidor].**
3. **Na coluna direita, clique em [Criar Solicitação de Certificado...].**
4. **Insira todas as informações e, em seguida, clique em [Próximo].**
5. **Em "Provedor de serviços de criptografia:", selecione um provedor e, em seguida, clique em [Próximo].**
6. **Clique em [...] e, em seguida, especifique um nome de arquivo para a solicitação de certificado.**
7. **Especifique um local para armazenar o arquivo e clique em [Abrir].**
8. **Feche o [Gerenciador do Serviços de Informações da Internet (IIS)] clicando em [Concluir].**

Autenticação LDAP

Especifique este método de autenticação quando utilizar o servidor LDAP para autenticar usuários que tenham as suas contas no servidor LDAP. Os usuários não podem ser autenticados se não tiverem as suas contas no servidor LDAP. O Catálogo de endereços armazenado no servidor LDAP pode ser registrado no equipamento, permitindo a autenticação do usuário sem primeiro utilizar o equipamento para registrar definições individuais no Catálogo de endereços. Quando utilizar a autenticação LDAP, para evitar que as informações da senha sejam enviadas sem criptografia pela rede, recomendamos que a comunicação entre o equipamento e o servidor LDAP seja criptografada via SSL. Você pode especificar no servidor LDAP se deseja ou não ativar o SSL. Para isso, você deve criar um certificado de servidor para o servidor LDAP. Para obter mais informações sobre como criar um certificado de servidor, consulte Pág. 47 "Criar o certificado de servidor". As configurações de SSL podem ser especificadas na definição do servidor LDAP.

Com o uso do Web Image Monitor, é possível ativar uma função para verificar se o servidor SSL é confiável.
Para mais informações sobre a especificação da autenticação LDAP utilizando o Web Image Monitor, consulte a Ajuda do Web Image Monitor.

Quando você seleciona a autenticação de texto simples, a autenticação simplificada LDAP é ativada. A autenticação simplificada pode ser executada com um atributo de usuário (como cn ou uid) em vez de DN.

Para ativar o Kerberos para a autenticação LDAP, é necessário registrar previamente um realm. Um realm deve ser configurado em letras maiúsculas. Para obter mais informações sobre o registro de um realm, consulte Connecting the Machine/ System Settings.

Importante

- Se utilizar autenticação LDAP, as informações do usuário registradas no servidor LDAP serão registradas automaticamente no Catálogo de endereços do equipamento. Mesmo que as informações do usuário registradas automaticamente no Catálogo de endereços do equipamento sejam editadas no equipamento, elas serão substituídas pelas informações do servidor LDAP quando a autenticação for efetuada.
- Com a autenticação LDAP, não é possível especificar limites de acesso para grupos registrados no servidor do diretório.
- Não utilize caracteres japoneses, chineses tradicionais, chineses simplificados ou coreanos de dois bytes quando inserir o nome de usuário ou a senha de login. Se você utilizar caracteres de dois bytes quando inserir o nome de usuário e a senha de login, não conseguirá fazer a autenticação usando o Web Image Monitor.
- Se você estiver usando o Active Directory na autenticação LDAP quando as autenticações Kerberos e SSL estiverem sendo usadas ao mesmo tempo, as informações do usuário não poderão ser obtidas.

- **Na autenticação LDAP, se nas definições do servidor LDAP a "Autenticação anônima" não estiver definida como "Proibir", os usuários que não têm conta no servidor LDAP poderão continuar a ter acesso.**
- **Se o servidor LDAP for configurado por meio do Windows Active Directory, a "Autenticação Anônima" pode estar disponível. Se a autenticação do Windows estiver disponível, recomendamos utilizá-la.**

Requisitos operacionais para a autenticação LDAP

Para especificar a autenticação LDAP, os seguintes requisitos devem ser atendidos:

- Configure a rede para que o equipamento possa detector o servidor LDAP.
- Quando SSL está sendo usado, o TLSv1 ou SSLv3 pode ser executado no servidor LDAP.
- Registre o servidor LDAP no equipamento.
- Para registrar o servidor LDAP, especifique as seguintes definições:
  - Nome do servidor
  - Base de pesquisa
  - Número porta
  - Comunicação SSL
  - Autenticação

    Selecione a autenticação Kerberos, DIGEST ou autenticação de texto simples.
  - Nome de usuário

    Não é necessário inserir o nome de usuário se o servidor LDAP suportar "Autenticação Anônima".
  - Senha

    Não é necessário inserir a senha se o servidor LDAP suportar "Autenticação anônima".

Para mais informações sobre como registrar um servidor LDAP, consulte Connecting the Machine/System Settings.

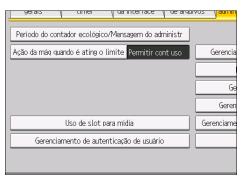
- Para saber que caracteres podem ser usados para nomes de usuários e senhas de login, consulte Pág. 19 "Caracteres que podem ser usados para nomes de usuários e senhas".
- No modo de autenticação simples LDAP, a autenticação falhará se a senha for deixada em branco. Para utilizar senhas em branco, contate seu representante técnico.
- Na primeira vez em que um usuário não registrado acessar o equipamento depois que a autenticação LDAP for especificada, ele será registrado no equipamento e poderá usar as funções disponíveis em "Funções disponíveis" durante a autenticação LDAP. Para limitar as funções disponíveis para cada usuário, registre cada usuário e a definição das "Funções disponíveis" correspondentes no Catálogo de endereços ou especifique as "Funções disponíveis" para cada

usuário registrado. A definição das "Funções disponíveis" é ativada quando o usuário acessa o equipamento.

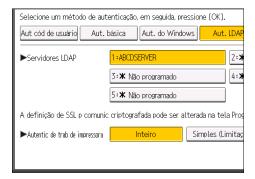
- A transmissão de dados entre o equipamento e o servidor KDC será criptografada se a autenticação Kerberos estiver ativada. Para obter mais informações sobre como especificar uma transmissão criptografada, consulte Pág. 165 "Definições de criptografia da autenticação Kerberos".

2

Antes de configurar o equipamento, certifique-se de que a autenticação de administrador esteja devidamente configurada em "Gerenciamento de autenticação de administrador".

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Gerenciamento de autenticação de usuário].**

6. **Selecione [Aut. LDAP].**

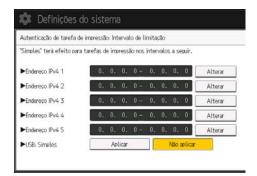
   Se não quiser ativar a autenticação de usuário, selecione [Desligado].

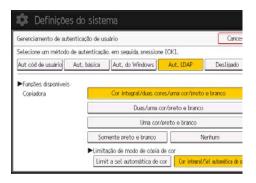
7. **Selecione o servidor LDAP a ser utilizado para a autenticação LDAP.**

8. **Selecione o nível de "Autenticação de trabalho de impressora".**

   Para obter uma descrição dos níveis de autenticação dos trabalhos da impressora, consulte Pág. 53 "Autenticação de trabalhos da impressora".

Se você selecionar [Inteiro] ou [Simples (Tudo)], vá para a etapa 12.

Se você selecionar [Simples (Limitação)], vá para a etapa 9.

9. **Pressione [Alterar] para "Intervalo de limitação".**
10. **Especifique o intervalo no qual [Simples (Limitação)] é aplicado à "Autentic trab impressora".**

Você pode especificar o intervalo do endereço IPv4 ao qual será aplicada essa definição.

11. **Pressione [Sair].**
12. **Pressione [▼Próximo].**
13. **Em "Funções disponíveis", selecione qual das funções do equipamento você deseja permitir.**

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

A autenticação LDAP será aplicada às funções selecionadas.

Os usuários só podem utilizar as funções selecionadas.

Para informações sobre como especificar as funções disponíveis a pessoas ou grupos, consulte Pág. 70 "Limitar as Funções disponíveis".

14. **Pressione [▼Próximo].**
15. **Pressione [Alterar] para "Atrib de nome de login".**

16. **Insira o atributo do nome de login e, em seguida, pressione [OK].**

    Utilize o atributo do nome de login como critério de pesquisa para obter informações sobre um usuário autenticado. É possível criar um filtro de pesquisa com base no atributo do nome de login, selecionar um usuário e, em seguida, obter as informações do usuário no servidor LDAP para que sejam transferidas para o Catálogo de endereços do equipamento.

    Para especificar vários atributos de login, coloque uma vírgula (,) entre eles. A pesquisa retornará resultados para um ou ambos os atributos.

    Além disso, se você colocar um sinal de igual (=) entre dois atributos de login (por exemplo: cn=abcde, uid=xyz), a pesquisa só retornará resultados que coincidam com os atributos. Essa função de pesquisa também pode ser aplicada quando a autenticação de texto não criptografado estiver especificada.

    Ao autenticar utilizando o formato DN, os atributos de login não precisam ser registrados.

    O método para selecionar o nome de usuário depende do ambiente do servidor. Verifique o ambiente do servidor e insira o nome do usuário correspondente.

17. **Pressione [Alterar] para "Atributo exclusivo".**
18. **Insira o atributo exclusivo e, em seguida, pressione [OK].**

    Especifique o atributo exclusivo do equipamento para fazer a correspondência das informações de usuário no servidor LDAP com as do equipamento. Dessa forma, se o atributo exclusivo de um usuário registrado no servidor LDAP corresponder ao de um usuário registrado no equipamento, ambos os casos serão tratados como se referissem ao mesmo usuário.

    Você pode inserir um atributo como “NúmeroSérie” ou “uid”. Você também pode inserir “cn” ou “NúmeroFuncionário”, desde que seja exclusivo. Se você não especificar o atributo exclusivo, será criada no equipamento uma conta com as mesmas informações de usuário, mas com um nome de usuário de login diferente.

19. **Pressione [OK].**
20. **Pressione a tecla [Login/Logout].**

    Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Autenticação de trabalhos da impressora

A autenticação do trabalho de impressão é uma função que aplica a autenticação do usuário nos trabalhos de impressão.

Os drivers PCL e PostScript3 dão suporte à autenticação de usuário. O driver PostScript3 suporta apenas autenticação do código do usuário.

Níveis de autenticação de trabalhos da impressora

O nível de segurança para "Inteiro" é o mais alto, seguido por "Simples (Limitação)", e na parte inferior, "Simples (Tudo)".

- Inteiro

  Selecione isso para autenticar todos os trabalhos de impressão e definições remotas.

  O equipamento autentica todos os trabalhos da impressora e as definições remotas, cancelando os trabalhos e as definições que apresentarem falha na autenticação.

  Para imprimir em um ambiente que não suporta autenticação, selecione [Simples (Tudo)] ou [Simples (Limitação)].

- Simples (Limitação)

  Selecione essa opção para restringir o intervalo de [Simples (Tudo)].

  O intervalo especificado pode ser impresso independentemente da autenticação. A autenticação será aplicada a endereços fora desse intervalo.

  Você pode especificar se [Simples (Tudo)] será aplicado ao endereço IPv4 do usuário. O intervalo de aplicação a endereços IPV6 pode ser configurada no Web Image Monitor.

- Simples (Tudo)

  Selecione essa opção se desejar imprimir com um driver de impressão ou dispositivo que não possa ser identificado pelo equipamento ou se a autenticação não for necessária para impressão.

  Os trabalhos da impressora e as definições sem informações de autenticação são executados sem serem autenticados.

  O equipamento autentica os trabalhos da impressora e as definições remotas que possuem informações de autenticação, cancelando os trabalhos e as definições que apresentarem falha de autenticação.

  Usuários não autorizados podem utilizar o equipamento desde que a impressão seja permitida sem a autenticação de usuário.

Tipos de trabalhos da impressora

Dependendo da combinação do nível de autenticação do trabalho da impressora e do tipo de trabalho na impressora, o equipamento pode não imprimir corretamente. Defina uma combinação adequada de acordo com o ambiente de funcionamento.

Quando a autenticação do usuário estiver desativada, a impressão ficará disponível para todos os tipos de trabalho.

Tipos de trabalhos de impressão: Um trabalho de impressão é especificado quando:

1. A caixa de seleção [Autenticação do usuário] é marcada no driver de impressão PCL ou no driver universal PCL.
2. As caixas de seleção [Autenticação do usuário] e [Com criptografia] são marcadas no minidriver PCL*.

    * A função de autenticação não pode ser usada com sistemas operacionais IA-64.
3. A caixa de seleção [Autenticação do usuário] é marcada no minidriver PCL.
4. A caixa de seleção [Autenticação do usuário] não é selecionada no driver PCL de impressão ou no minidriver PCL*.

    * A função de autenticação não pode ser usada com sistemas operacionais IA-64.
5. O Código de usuário é inserido usando o driver PostScript 3 de impressão ou o driver universal PS3.

    Isso também se aplica à impressão de recuperação/paralela utilizando um driver de impressão PCL que não suporta autenticação.
6. O Código de usuário não é inserido usando o driver de impressão PostScript 3 ou o driver universal PS3. Isso também se aplica à impressão de recuperação/paralela utilizando um driver de impressão PCL que não suporta autenticação.
7. Um trabalho de impressão ou arquivo PDF é enviado de um computador host sem driver de impressão e é impresso via LPR.
8. Um arquivo PDF é impresso via ftp. A autenticação pessoal é executada através da ID do usuário e da senha usadas para fazer login através de ftp. No entanto, a ID do usuário e a senha não estão criptografadas.

Níveis de autenticação de trabalhos da impressora e tipos de trabalhos da impressora

Autentic de trab de impressora: Chave criptografia do driver: Nível cript	Simples (Tudo): Criptograf ia simples	Simples (Tudo): DES	Simples (Tudo): AES	Inteiro: Criptograf ia simples	Inteiro: DES	Inteiro: AES
Trabalho da impressora Tipo 1	C*1	C*1	C*1	C*1	C*1	C*1

Autentic de trab de impressora: Chave criptografia do driver: Nível cript	Simples (Tudo): Criptografia simples	Simples (Tudo): DES	Simples (Tudo): AES	Inteiro: Criptografia simples	Inteiro: DES	Inteiro: AES
Trabalho da impressora Tipo 2	C*1	C*1	X*1	C*1	C*1	X*1
Trabalho da impressora Tipo 3	B	X*1	X*1	B	X*1	X*1
Trabalho da impressora Tipo 4	X	X	X	X	X	X
Trabalho da impressora Tipo 5	A	A	A	B	B	B
Trabalho da impressora Tipo 6	A	A	A	X	X	X
Trabalho da impressora Tipo 7	A	A	A	X	X	X
Trabalho da impressora Tipo 8	B	B	B	B	B	B

*1 A impressão com autenticação de código de usuário é classificada como B.

A: É possível imprimir independentemente da autenticação de usuários.

B: É possível imprimir caso a autenticação de usuário seja bem-sucedida. Se a autenticação de usuário falhar, o trabalho de impressão é redefinido.

C: É possível imprimir caso a autenticação do usuário seja bem-sucedida e a "Chave criptogr driver" do driver de impressão seja a mesma do equipamento.

X: Não é possível imprimir independentemente da autenticação de usuário, e o trabalho de impressão é redefinido.

- Para informações sobre "Chave criptografia do driver: Nível cript", consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

Comando "authfree"

Se [Simples (Limitação)] estiver selecionado em uma autenticação de trabalho de impressão, o comando telnet authfree pode ser usado para especificar exceções à autenticação do trabalho de impressão.

Para obter informações sobre o nome de usuário e a senha de login para entrar no telnet, pergunte ao administrador. Para obter informações sobre como fazer login e usar o telnet, consulte Connecting the Machine/ System Settings.

Visualizar definições

```
msh> authfree
```

Se a exclusão da autenticação do trabalho de impressão não for especificada, não será possível exibir o controle de exclusão de autenticação.

Definições de endereço IPv4

```
msh> authfree "ID" range "start-address" "end-address"
```

Definições de endereço IPv6

```
msh> authfree "ID" range6 "start-address" "end-address"
```

Definições de máscara de endereço IPv6

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

Inicialização do controle de exclusão de autenticação

```
msh> authfree flush
```

- Nos ambientes IPv4 e IPv6, até 5 intervalos de acesso podem ser registrados e selecionados.

Registro automático no Catálogo de endereços

As informações pessoais de usuários que efetuam login via autenticação Windows ou LDAP são automaticamente registradas no Catálogo de endereços. Outras informações poderão ser especificadas copiando-as de outros usuários registrados.

Itens do Catálogo de endereços registrados automaticamente

- Login do usuário
- Senha
- N° de registro
- Nome*1
- Exibição da tecla*1
- Endereço de e-mail*2
- Proteger arquivo(s)

  Permissões para usuários/grupos*3

*1 Se essas informações não puderem ser obtidas, o nome de usuário de login será registrado nesse campo.

*2 Se essas informações não puderem ser obtidas, o registro automático não funcionará.

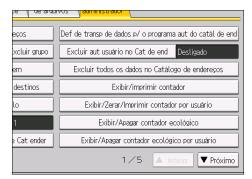
*3 Se [Def de transp de dados p/ o programa aut do catál de end] for definido como [Transferir dados], essa opção terá prioridade.

- Você pode excluir contas de usuários antigos automaticamente ao executar o registro automático se a quantidade de dados registrados no Catálogo de endereços tenha atingido o limite.
  Para mais informações, consulte Pág. 248 "Gerenciar o Catálogo de endereços ".

Def de transp de dados p/ o programa aut do catál de end

As informações não registradas automaticamente no Catálogo de endereços podem ser copiadas de um usuário já registrado e, em seguida, registradas.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**

4. **Pressione [Def de transp de dados p/ o programa aut do catál de end].**

5. **Pressione [Transferir dados]**
6. **Use as teclas numéricas para inserir o número do registro no Catálogo de endereços para aplicar a definição especificada e, em seguida, pressione [#].**
7. **Pressione [OK].**
8. **Pressione a tecla [Login/Logout].**

   Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Função Bloqueio de usuário

Se uma senha incorreta for inserida várias vezes, a função Bloqueio de usuário evitará novas tentativas de login com o mesmo nome de usuário de login. Mesmo que o usuário bloqueado insira a senha correta posteriormente, a autenticação falhará e o equipamento não poderá ser utilizado até que o período de bloqueio termine ou um administrador ou supervisor desative o bloqueio.

Para utilizar a função de bloqueio para autenticação de usuário, o método de autenticação deve estar definido como autenticação básica. Com outros métodos de autenticação, a função de bloqueio protege apenas as contas do supervisor e do administrador, e não as contas dos usuários gerais.

Itens da definição de bloqueio

As definições da função de bloqueio podem ser efetuadas utilizando o Web Image Monitor.

Item da definição	Descrição	Valores da definição	Definição padrão
Bloqueio	Especifique se deseja ou não ativar a função de bloqueio.	• Ativo • Inativo	Inativo
Número de tentativas antes do bloqueio	Especifique o número de tentativas de autenticação permitidas antes da aplicação do bloqueio.	1-10	5
Timer de liberação de bloqueio	Especifique se deseja ou não cancelar o bloqueio após um período específico.	• Ativo • Inativo	Inativo
Bloquear usuário para	Especifique o número de minutos antes do cancelamento do bloqueio.	1-9999 min.	60 min.

Privilégios para desbloqueio

Administradores com privilégios de desbloqueio:

Usuário bloqueado	Administrador de desbloqueio
Usuário geral	Administrador de usuário

Usuário bloqueado	Administrador de desbloqueio
Administrador de usuários, administrador de rede, administrador de arquivos, administrador do equipamento	Supervisor
Supervisor	Administrador de equipamento

Especificar a função Bloqueio de usuário

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Política de bloqueio de usuário] em "Segurança".**
4. **Defina "Bloqueio" como [Ativo].**
5. **No menu, selecione o número de tentativas de login permitidas antes da aplicação do bloqueio.**
6. **Após o bloqueio, se desejar cancelá-lo depois de um tempo especificado, defina "Lockout Release Timer" (Timer de desbloqueio) como [Ativo].**
7. **No campo "Lock Out User for" (Bloquear usuário por), insira o número de minutos até a desativação do bloqueio.**
8. **Clique em [OK].**

   A Política de bloqueio de usuário está definida.
9. **Faça logout.**

Cancelar o bloqueio de senha

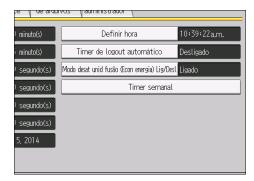
1. **Faça login como administrador de usuários no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Catálogo de endereços].**
3. **Selecione a conta do usuário bloqueado.**
4. **Clique em [Entrada detalhada] e em seguida clique em [Alterar].**
5. **Defina opção "Bloqueio" como [Inativo] em "Informações de autenticação".**
6. **Clique em [OK].**
7. **Faça logout.**

- O bloqueio de senha do administrador e supervisor pode ser cancelado desligando o equipamento e religando-o ou cancelando a definição em [Programar/Alterar administrador] no menu [Configuração] do Web Image Monitor.

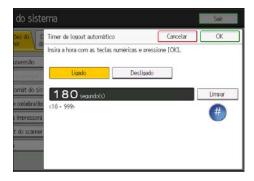
Logout automático

Depois de fazer o login, o equipamento faz o logout automaticamente se você não usar o painel de controle após um tempo determinado.

Esta função é chamada "Logout automático". Especifique o período de tempo que o equipamento deve aguardar antes de executar o Logout automático.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Definições de timer].**
4. **Pressione [Timer de logout automático].**

5. **Selecione [Ligado].**

   Se não quiser especificar [Timer de logout automático
   ], selecione [Desligado].

6. **Insira "10" a "999" (segundos) utilizando as teclas numéricas e, em seguida, pressione [#].**

   Em caso de erro, pressione [Limpar].

7. **Pressione [OK].**

8. **Pressione a tecla [Login/Logout].**

   Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

- Você pode especificar as definições de Logout automático para Web Image Monitor em [Página da Web]. Para mais informações, consulte a Ajuda do Web Image Monitor.

Autenticação Utilizando um Dispositivo Externo

Para efetuar a autenticação usando um dispositivo externo, consulte o manual do dispositivo.

Para obter mais informações, contate o seu consultor comercial.

3. Restringir o uso do equipamento

Este capítulo explica como restringir o uso do equipamento pelo usuário.

Restringir o uso de lista de destinos

O uso da lista de destino pode ser restrito separadamente na função do scanner.

Restringir uso de destinos

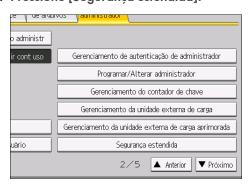
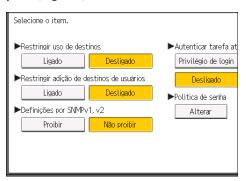
É possível proibir o envio de documentos digitalizados para endereços não registrados no Catálogo de endereços. Ativando essa opção, é possível proibir que os usuários insiram manualmente endereços de e-mail ou destinos de pastas.

Restringir adição de destinos de usuários

Ao usar [Dest progr], é possível proibir que os endereços inseridos manualmente para o envio de documentos digitalizados sejam registrados no Catálogo de endereços. Com essa definição, apenas o administrador de usuários pode cadastrar novos usuários no Catálogo de endereços e alterar senhas e outras informações dos usuários já cadastrados. Além disso, mesmo que essas funções sejam definidas como [Ligado], o usuário registrado como destino pode alterar sua senha. Somente o administrador pode alterar itens diferentes da senha.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Segurança estendida].**

6. **Pressione [▼Próximo].**

3

7. **Configure "Restringir uso de destinos" ou "Restringir adição de destinos de usuários" para [Ligado].**

Se você definir "Restringir uso de destinos" como [Ligado], "Restringir adição de destinos de usuários" não aparecerá.

8. **Pressione [OK].**
9. **Pressione a tecla [Login/Logout].**

Aparece uma mensagem de confirmação. Se você pressionar [Sim], o logout é feito automaticamente.

Evitar alterações nas definições do administrador

Limitar as definições que podem ser alteradas por cada administrador.

As definições que podem ser feitas neste equipamento variam de acordo com o tipo de administrador, permitindo que a variedade de operações que podem ser executadas seja compartilhada pelos administradores.

Os seguintes administradores estão definidos para este equipamento:

- Administrador de usuário
- Administrador de equipamento
- Administrador de redes
- Administrador de arquivos

Para obter informações sobre as definições que podem ser especificadas por cada administrador, consulte Pág. 285 "Lista de privilégios de operações em definições".

Registre os administradores antes de utilizar o equipamento. Para obter instruções sobre como registrar administradores, consulte Pág. 17 "Registro e alteração de administradores".

Proibir que usuários alterem as definições

É possível proibir que usuários alterem as definições feitas pelos administradores.

Selecione o item em "Definições disponíveis" em "Gerenciamento de autenticação de administrador" para evitar essas
alterações.

Para obter mais detalhes sobre os itens que podem ser selecionados em "Definições disponíveis", consulte Pág. 14 "Configurar a autenticação de administrador".

Especificar a definição Proteger menu

Proteger menu permite limitar as permissões de acesso do usuário às definições no menu Ferramentas do usuário, exceto para as Definições do sistema. Essa definição pode ser utilizada, independentemente de autenticação do usuário. Para especificar a definição Menu Protect (Proteção de menus), habilite previamente a autenticação de administrador para o administrador do equipamento. Para obter mais informações sobre como definir a autenticação do administrador, consulte Pág. 14 "Configurar a autenticação de administrador". Para obter uma lista com as definições que os usuários podem especificar de acordo com o nível de proteção dos menus, consulte Pág. 285 "Lista de privilégios de operações em definições".

Se desejar ativar "Proteger menu", defina como [Nível 1] ou [Nível 2]. Selecione [Nível 2] para impor restrições mais fortes às permissões de acesso dos usuários às definições do equipamento.

Se desejar desativar a função "Proteger menu", defina-a como [Desligado].

Função de cópia

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Recurso de copiadora/servidor de documentos].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Proteger menu].**
5. **Selecione o nível de proteção do menu e, em seguida, pressione [OK].**
6. **Faça logout.**

Função de impressora

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Recursos da impr].**
3. **Pressione [Gerenciamento de dados].**
4. **Pressione [Proteger menu].**
5. **Selecione o nível de proteção do menu e, em seguida, pressione [OK].**
6. **Faça logout.**

Função de scanner

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Recursos de scanner].**

3. **Pressione [Definições iniciais].**
4. **Pressione [Proteger menu].**
5. **Selecione o nível de proteção do menu e, em seguida, pressione [OK].**
6. **Faça logout.**

Evitar que usuários registrem/alterem programas

Habilitando a definição Menu Protect (Proteção de menus), você pode evitar que usuários registrem ou alterem programa. Quando essa definição é habilitada, o administrador do equipamento registra e altera programas.

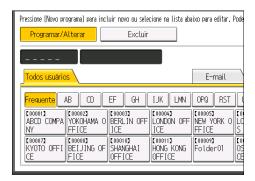
Para obter mais informações sobre registro e alteração de programas, consulte Convenient Functions.

Limitar as Funções disponíveis

Para prevenir operações não autorizadas, é possível especificar quem está autorizado a acessar cada função do equipamento.

Especifique as funções disponíveis para usuários registrados. Ao fazer essa definição, você pode limitar as funções disponíveis aos usuários.

Você pode estabelecer limitações quanto ao uso da copiadora, Servidor de documentos, scanner, funções da impressora e recursos estendidos.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário.**

4. **Pressione [Inform Aut.].**

5. **Pressione [▼Próximo] duas vezes.**

6. **Em "Funções disponíveis", selecione as funções que deseja especificar.**

Se a função que deseja selecionar não for exibida, pressione [▼Próximo].

7. **Pressione [OK].**

8. **Faça logout.**

Restringir o acesso ao slot para mídia

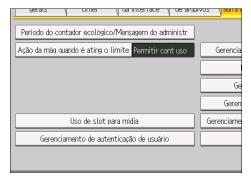
Especifique no painel de controle se deseja permitir que usuários usem os slots de mídia. Com essa definição, é possível restringir o armazenamento dos arquivos digitalizados a um dispositivo de memória removível. Também é possível restringir a impressão de arquivos armazenados em um dispositivo de memória removível.

1. Faça login como administrador do equipamento no painel de controle.

2. Pressione [Definições do sistema].

3. Pressione [Ferramentas admin].

4. Pressione [▼Próximo].

5. Pressione [Uso de slot para mídia].

6. Para restringir o armazenamento de arquivos em um dispositivo de memória removível, pressione [Proibir] em Armazenar no disp de mem.

7. Para restringir a impressão de arquivos armazenados em um dispositivo de memória removível, pressione [Proibir] em Imprimir a partir do disp de armaz de mem.

8. Pressione [OK].

9. Faça logout.

- Se você selecionar [Proibir] em "Armazenar no disp de mem", o botão [Armazenar no disp de mem] não aparecerá na tela Armazenar arquivo da função de scanner.
- Se você selecionar [Proibir] em "Imp a partir do disp de armaz de mem", o botão [Imp a partir do disp de armaz de mem] não aparecerá na tela inicial da função de impressora.

Gerenciar volume de impressão por usuário

Esta função especifica o limite de volume de impressão de cada usuário. Se o número do volume de impressão que cada usuário pode especificar alcançar o máximo, os trabalhos de impressão são cancelados e uma mensagem indicando que o volume de impressão chegou ao máximo é exibida.

Volume de impressão

O volume de impressão é calculado multiplicando-se o número de páginas por uma contagem de unidade.

A contagem de unidade pode ser especificada de acordo com as condições de impressão. Por exemplo, se 1 página for impressa com uma contagem de unidade igual a 10, o volume de impressão é 10.

O volume de impressão é controlado para cada usuário.

Itens da definição

Item	Explicação	Definição
Ação da máq quando é ating o limite	Especifique se deseja limitar os volumes de impressão e o método para limitar impressões. • Parar trabalho Quando o volume de impressão chega ao máximo, o trabalho atual e os trabalhos em espera são cancelados. • Concluir trab e limite Quando o volume de impressão chega ao máximo, o trabalho atual é concluído, mas os trabalhos em espera são cancelados. • Permitir continuar uso Não especifica limite de volumes de impressão.	• Parar trabalho • Concluir trab e limite • **Permitir continuar uso** (definição padrão)

Item	Explicação	Definição
Lim de uso de vol de impressão: Def de cont de unidade	É possível especificar os limites do volume de impressão por usuário com base nas 8 condições a seguir. • Copiadora:Cor:A3/DLT • Copiadora:Preto e Bco:A3/DLT • Copiadora:Cor:Outras • Copiadora: Preto e bco:Outras • Impressora:Cor:A3/DLT • Impres:Preto e Bco:A3/DLT • Impressora:Cor:Outras • Impres: Preto e bco:Outras	0 a 200 (A contagem de unidade por página padrão para todas as condições de impressão é 1.)

3

Observação sobre os limites de volume de impressão

Caso o seguinte aconteça, não é possível imprimir:

- O nome de usuário de login ou o código de usuário registrado no Catálogo de endereços é alterado embora o usuário tenha feito login e esteja autenticado.

Se ocorrer a seguinte situação, o gerenciamento de volume de impressão não funcionará corretamente:

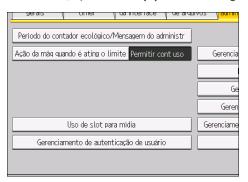
- Com a autenticação do Windows ou LDAP, um usuário faz login na mesma conta utilizando vários nomes de usuário, sendo que esses vários nomes de usuário estão registrados no Catálogo de endereços como usuários separados.

Limites de volume de impressão não são aplicados às seguintes operações:

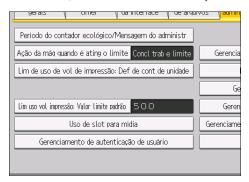
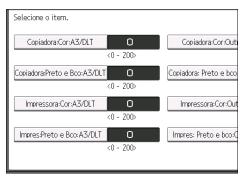
- Impressão por meio de um sistema operacional que não suporta o método de autenticação atual

Especificar limitações para volume de impressão

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**

5. **Pressione [Ação da máq quando é ating o limite].**

6. **Selecione [Parar trabalho] ou [Concluir trab e limite] e, em seguida, pressione [OK].**

   Se não quiser limitar os volumes de impressão, selecione [Permitir continuar uso].

7. **Pressione [Lim de uso de vol de impressão: Def de cont de unidade].**

8. **Para cada condição de impressão, utilize as teclas numéricas para inserir uma contagem de unidade por página entre "0" e "200" e, em seguida, pressione [#].**

   Se você especificar "0" para a condição de impressão, não será aplicada nenhum limite de volume aos trabalhos que corresponderem a essa condição.

9. **Pressione [OK].**

10. **Faça logout.**

- Os limites de volume de impressão também podem ser especificados em [Lim de uso de vol de impressão] em "Configuração" em Web Image Monitor.

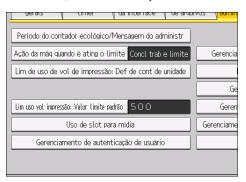
Restrições quando a autenticação do código de usuário está ativada

Quando a autenticação do código de usuário está ativada, as restrições a seguir se aplicam às definições de limite do volume de impressão:

- Se [Controle de PC] estiver selecionado para a função de impressora, os valores especificados para as unidades de uso de volume de impressão podem não ser aplicados aos contadores de impressão do usuário. Não selecione [Controle de PC] se quiser especificar os limites do volume de impressão quando a autenticação do código de usuário está ativada.
- Na autenticação básica, Windows e LDAP, os números exibidos no canto inferior esquerdo do painel de controle indicam os volumes totais que o administrador especifica para o usuário imprimir. Na autenticação do código de usuário, os usuários por si mesmos não podem verificar o volume de impressão total nem pelo painel de controle nem pelo Web Image Monitor. Neste caso, os usuários precisam perguntar aos administradores o volume total de impressão.
- Nenhum dado de registro do limite de uso da impressão é registrado no Registro de trabalho ou Registro de acesso.
- Dependendo das definições configuradas para a autenticação do código de usuário, os usuários poderão efetuar impressões antes de fazer login, independentemente dos limites de volume de impressão definida pelo administrador. Restrinja todas as funções via "Funções para restringir" em [Aut cód de usuário] em [Gerenciamento de autenticação de usuário].

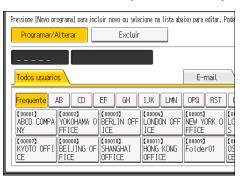
Especificar a contagem de utilização máxima padrão

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**

5. **Pressione [Lim uso vol impressão: Valor lim padrão].**

A opção [Lim uso vol impressão: Valor lim padrão] não é exibida se você selecionou [Permitir continuar uso] em "Ação da máq quando é ating o limite".

6. **Use as teclas numéricas para inserir um valor entre "0" e "999.999" como o volume de impressão máximo e, em seguida, pressione [#].**
7. **Pressione [OK].**
8. **Faça logout.**

Especificar a contagem de utilização máxima por usuário

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário cujo volume de impressão máximo você deseja especificar.**

4. **Pressione [Inform Aut.].**

5. **Pressione [▼Próximo] 4 vezes.**
6. **Pressione [Limitar] em "Vol imp Limit de uso.".**

"Limite uso volume de impressão" não é exibido se você selecionou [Permitir continuar uso] em "Ação da máq quando é ating o volume".

Se não pretende especificar os limites de volume de impressão, pressione [Não limitar].

7. **Pressione [Alterar] e use as teclas numéricas para inserir um valor entre "0" e "999.999" como o volume de impressão máximo disponível e, em seguida, pressione [#].**

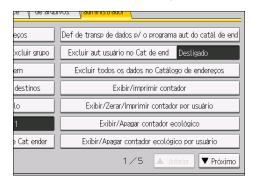
Um usuário cujo volume de impressão máximo seja "0" só pode imprimir trabalhos cujas condições de impressão coincidam com um valor de unidade de "0".

8. **Pressione [OK].**
9. **Faça logout.**

- O volume de impressão máximo para cada usuário também pode ser especificado no [Catálogo de endereços] no Web Image Monitor.

Verificar volume de impressão por usuário

Esse procedimento pode ser gerenciado por qualquer administrador.

1. **Faça login como administrador no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Exibir/Zerar/Imprimir contador por usuário].**

5. **Pressione [Uso de vol de imp].**

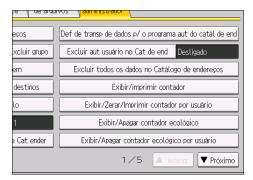
Os limites de volume de impressão e volumes de impressão total por cada usuário são exibidos.

6. **Faça logout depois de confirmar as definições.**

- Os usuários autorizados e o administrador de usuários também podem utilizar o [Catálogo de endereços] no Web Image Monitor para verificar os contadores de uso do volume de impressão de cada usuário.

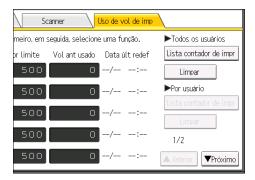
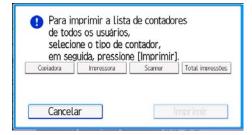
Imprimir uma lista de contadores de uso de volume de impressão

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**

4. **Pressione [Exibir/Zerar/Imprimir contador por usuário].**

5. **Pressione [Uso de vol de imp].**

   Uma lista dos contadores de uso de volume de impressão de cada usuário é exibida.

   Para selecionar todos os usuários apresentados na página, pressione [Selecionar todos na página].

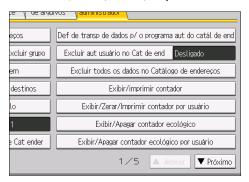
6. **Para imprimir uma lista dos contadores de uso do volume de cada usuário, pressione [Lista contador de impr] em Todos os usuários. Para imprimir uma lista dos contadores de uso do volume apenas dos usuários selecionados, selecione os usuários cujos contadores deseja imprimir e, em seguida, pressione [Lista dos contadores de impressão] em Por usuário.**

7. **Selecione o contador que deseja imprimir na lista e, em seguida, pressione [Imprimir].**

8. **Faça logout.**

- As listas de contadores de uso do volume de impressão podem ser impressas apenas se for inserido papel com os seguintes tamanhos na bandeja de papel: A4, 8 $^1/_2$ × 11 pol, B4, 8 $^1/_2$ × 14 pol, A3 ou 11 × 17 pol.

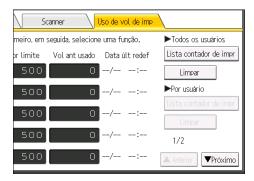
Redefinir os contadores de uso do volume de impressão

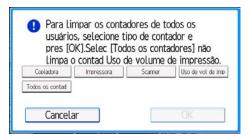
Quando o contador do volume de impressão de cada usuário é redefinido ou o limite de volume de impressão de cada usuário é aumentado, o usuário pode imprimir além do permitido.

3

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Exibir/Zerar/Imprimir contador por usuário].**

5. **Pressione [Uso de vol de imp].**

   Uma lista dos contadores de uso de volume de impressão de cada usuário é exibida.

6. **Para redefinir os contadores de uso do volume de impressão de cada usuário, pressione [Limpar] em Todos usuár. Para redefinir os contadores de uso do volume de impressão apenas dos usuários selecionados, selecione os usuários cujos contadores deseja redefinir e, em seguida, pressione [Limpar] em Por usuário.**

Para selecionar todos os usuários apresentados na página, pressione [Selecionar todos na página].

7. **Selecione [Uso de vol de imp] e, em seguida, pressione [OK].**

8. **Faça logout.**

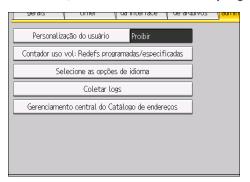
- Você também pode utilizar o [Catálogo de endereços] no Web Image Monitor para redefinir os contadores de uso do volume de impressão. No entanto, se pretende redefinir os contadores de uso do volume de impressão de todos os usuários simultaneamente, utilize o painel de controle.

Configuração da função de redefinição automática

O contador de volume de impressão pode ser redefinido em um tempo específico.

Opções	Detalhes
Todo mês	Redefine o volume de impressão na hora/data especificada de cada mês.
Especificar data	Redefine o volume de impressão (apenas uma vez) na hora/data especificada.
Especificar ciclo	Redefine o contador após o intervalo especificado a partir de uma data de referência e, posteriormente, o redefine depois de decorrido o mesmo intervalo.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 4 vezes.**

5. **Pressione [Contador uso vol: Redefs programadas/especificadas].**

6. **Selecione uma das opções: [Todo mês], [Especificar data] e [Especificar ciclo].**
7. **Configure as condições.**
8. **Pressione [OK].**
9. **Faça logout.**

- Se o equipamento estiver desligado na hora e data especificadas, o volume de impressão será redefinido quando ele for ligado.
- Ao selecionar uma data em [Todo mês], como o dia 31, que alguns meses têm e outros não, o volume de impressão será redefinido para 0:00 no primeiro dia do mês seguinte ao mês que não tem o dia 31.

4. Evitar vazamento de informações do equipamento

Este capítulo descreve como proteger informações caso estejam armazenadas na memória ou no disco rígido do equipamento.

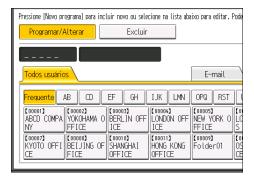
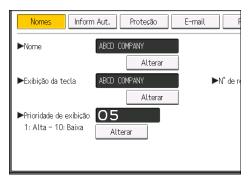
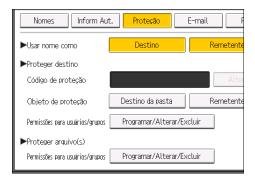
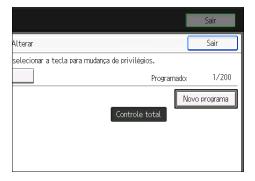
Proteger o Catálogo de endereços

Você pode especificar a quem é permitido o acesso aos dados no Catálogo de endereços. Para proteger os dados de usuários não autorizados, também é possível criptografar os dados no Catálogo de endereços.

Especificar permissões de acesso ao Catálogo de endereços

As permissões de acesso podem ser especificadas pelos usuários registrados no Catálogo de endereços, usuários com privilégios de controle total e administrador de usuário.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário para o qual você deseja alterar a permissão de acesso.**

4. **Pressione [Proteção].**

5. **Pressione [Programar/Alterar/Excluir] para "Permissões para usuários/grupos", em "Proteger destino".**

6. **Pressione [Novo progr].**

7. **Selecione os usuários ou grupos para os quais deseja aplicar as permissões de acesso.**

   É possível selecionar usuários múltiplos.

   Pressione [Todos usuários] para selecionar todos os usuários.

8. **Pressione [Sair].**

9. **Selecione o usuário a quem deseja atribuir permissões de acesso e, em seguida, especifique a permissão.**

   Selecione uma das seguintes opções:[Somente leitura], [Editar], [Editar/Excluir] ou [Controle total].

10. **Pressione [Sair].**
11. **Pressione [OK].**
12. **Faça logout.**

- Permissões de acesso "Editar", "Editar/Excluir", e "Controle total" permitem que os usuários executem operações que podem resultar na perda ou alteração de informação sigilosa. Recomendamos que você conceda apenas a permissão "Somente leitura" para os usuários gerais.

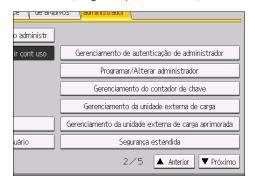
Criptografar dados no Catálogo de endereços

Importante

- O equipamento não pode ser utilizado durante a criptografia.

O tempo para criptografar os dados no Catálogo de endereços depende do número de usuários registrados.

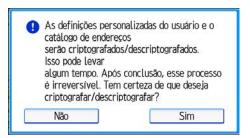
A criptografia dos dados no Catálogo de endereços pode demorar muito.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Segurança estendida].**

6. **Pressione [Ligado] para "Criptogr Defs personaliz do usuár e Cat endereços".**
7. **Pressione [Alterar] para "Chave de criptografia".**

8. **Insira a chave de criptografia e, em seguida, pressione [OK].**

   Insira a chave de criptografia utilizando até 32 caracteres alfanuméricos.

9. **Pressione [Criptografar/Descript].**

10. **Pressione [Sim].**

   Não desligue a alimentação principal durante a criptografia, pois isso pode danificar os dados.

   Se você pressionar [Parar] durante a criptografia, os dados não serão criptografados.

   Se você pressionar [Parar] durante a descriptografia, os dados não serão descriptografados.

   Normalmente, quando a criptografia é concluída, "A criptografia/descriptografia foi concluída com êxito. Pressione [Sair]." é exibido.

11. **Pressione [Sair].**

12. **Pressione [OK].**

13. **Faça logout.**

- Se você registrar mais usuários depois de criptografar os dados no Catálogo de endereços, os dados deles também são criptografados.
- O backup dos dados do livro de endereços guardados no SD card é encriptado. Para obter mais informações sobre como fazer backup e restaurar o Catálogo de endereços utilizando um cartão SD, consulte Conexão da máquina/Definições do sistema.

Criptografar dados no equipamento

⚠CUIDADO

- Mantenha cartões SD ou dispositivos USB de memória flash fora do alcance de crianças. Se uma criança engolir acidentalmente um cartão SD ou um dispositivo USB de memória flash, procure um médico imediatamente.

Mesmo se o dispositivo de memória ou o disco rígido forem roubados, você pode evitar perda de dados ao criptografar os dados no equipamento, como o Catálogo de endereços, dados de autenticação e arquivos

Quando a criptografia estiver ativada, todos os dados armazenados posteriormente no equipamento serão criptografados.

Você pode também optar por criptografar ou excluir os dados atualmente armazenados no equipamento.

O algoritmo de criptografia é AES-256.

Dados que são criptografados

Essa função criptografa dados armazenados na NVRAM (memória que permanece ativa mesmo depois que equipamento é desligado) do equipamento e no disco rígido.

Os seguintes dados são criptografados:

NVRAM

- Informações de definições do sistema
- Informações de definição da interface de rede
- Informações de código de usuário
- Informações do contador

Disco rígido

- Catálogo de endereços
- Programa/log do aplicativo Embedded Software Architecture
- Logs (log de trabalhos/log de acessos/log ecológico)
- Mensagens de e-mail enviadas/recebidas
- Fontes registradas
- Trabalhos em spool
- Miniaturas dos arquivos armazenados
- Documentos armazenados
- Carimbos registrados

Tipo de criptografia

Especifique se deseja criptografar os dados existentes e mantê-los no disco rígido ou excluí-los (formatar) A criptografia demora se houver uma grande quantidade de dados a armazenar. Os dados NVRAM não serão excluídos (inicializados)

Definição	Dados a serem armazenados	Dados a serem inicializados	Tempo necessário
Som dados sist de arq	• Catálogo de endereços • Programa/log do aplicativo Embedded Software Architecture • Logs (log de trabalhos/log de acessos/log ecológico) • Mensagens de e-mail enviadas/recebidas • Fontes registradas • Trabalhos em spool • Miniaturas dos arquivos armazenados	• Documentos armazenados (documentos armazenados no Servidor de documentos e arquivos de Impressão bloqueada/arquivos de Impressão de teste/arquivos de Impressão armazenada/ arquivos de Reter impressão) • Carimbos registrados	Aproximadamente 3 horas
Todos os dados	Todos os dados: Dados a serem armazenados ou não quando [Somente dados do sistema de arquivos] é especificado	Nenhum	Aproximadamente 7 horas e 45 minutos
Formatar todos os dados	Nenhum	Todos os dados: Dados a serem armazenados ou não quando [Somente dados do sistema de arquivos] é especificado	Muitos minutos

4

Observações para ativar as configurações de criptografia

- Se você utilizar o aplicativo Embedded Software Architecture ou App2Me, especifique [Som dados sist de arq] ou [Todos os dados].
- Observe que as definições do equipamento não retornarão ao padrão do sistema mesmo que [Formatar todos os dados], [Som dados sist de arq] ou [Todos os dados] tenha sido especificado.

Restaurar dados

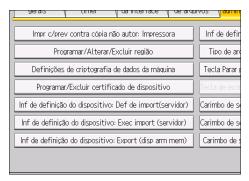
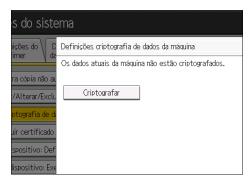
- Para transferir dados para um novo equipamento, restaure os dados criptografados. Para obter mais detalhes, contate o seu representante de serviços.
- A chave de criptografia utilizada para a criptografia de dados é necessária para restaurar os dados.
- Você pode especificar se deseja imprimir a chave de criptografia ou armazená-la em um cartão SD.
- Você pode alterar a chave de criptografia posteriormente.

Ativar as definições de criptografia

Importante

- Não é possível utilizar o equipamento durante a criptografia de dados.
- Após o início do processo de criptografia, não é possível pará-lo. Certifique-se de que o equipamento não seja desligado durante o processo de criptografia. Se o equipamento for desligado durante a criptografia, o disco rígido será danificado e os dados contidos nele ficarão inutilizados.
- É necessária a chave de criptografia para a recuperação de dados se o equipamento apresentar defeito. Certifique-se de armazenar a chave de criptografia de modo seguro para a recuperação de dados de backup.
- A criptografia começa depois que você termina o procedimento no painel de controle e reinicia o equipamento, desligando-o e religando-o. Se as funções de Apagar toda a memória e de criptografia estiverem especificadas, a criptografia inicia depois que os dados armazenados no disco rígido forem substituídos e o equipamento for reiniciado, desligando-o e ligando-o.
- Se você usar simultaneamente Apagar toda a memória e a criptografia e selecionar a opção para sobrescrever três vezes para "Números aleatórios", o processo levará até 13 horas. Criptografar novamente a partir de um estado já criptografado leva a mesma quantidade de tempo.
- A função "Apagar toda a memória" também apaga todas as definições de segurança do equipamento, deixando inoperante a administração do equipamento e dos usuários. Certifique-se de que os usuários não armazenem nenhum dado no equipamento após a conclusão de "Apagar toda a memória".

- A reinicialização será mais rápida se não existirem dados a serem transferidos para o disco rígido e se a criptografia estiver definida como [Formatar todos os dados], mesmo que todos os dados no disco rígido forem formatados. Antes de executar a criptografia, recomendamos que faça um backup dos dados importantes, como o Catálogo de endereços e todos os dados armazenados em Servidor documentos.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Definições de criptografia de dados da máquina].**

6. **Pressione [Criptografar].**

7. **Selecione os dados que serão transferidos para o disco rígido e o que não deve ser excluído.**

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Somente dados do sistema de arquivos]. Para excluir todos os dados, selecione [Formatar todos os dados].

8. **Especifique como realizar o backup da chave de criptografia.**

   Caso tenha selecionado [Save to SD Card] (Salvar no cartão SD), insira um cartão SD no slot de mídia na parte lateral do painel de controle e pressione [OK] para fazer o backup da chave de criptografia de dados da máquina.

Para obter informações sobre como manusear e inserir o cartão SD, consulte Getting Started.

Se você selecionou a opção [Imprimir em pap], pressione a tecla [Iniciar] e imprima a chave de criptografia de dados do equipamento.

9. **Pressione [OK].**
10. **Pressione [Sair].**
11. **Pressione [Sair].**
12. **Faça logout.**
13. **Desligue o equipamento e, em seguida, religue-o novamente.**

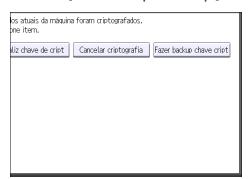
    O equipamento começará a converter os dados na memória depois que você ligá-lo. Aguarde até que a mensagem "Conversão de memória concluída. Desligue a chave de energia principal." seja exibida, em seguida desligue a chave de energia principal novamente.

    Para obter informações sobre como desligar a alimentação principal, consulte Getting Started.

Fazer backup da chave de criptografia

Você pode realizar o backup da chave de criptografia sem alterar a definição de criptografia.

- É necessária a chave de criptografia para a recuperação de dados se o equipamento apresentar defeito. Certifique-se de armazenar a chave de criptografia de modo seguro para a recuperação de dados de backup.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Definições de criptografia de dados da máquina].**
6. **Pressione [Fazer backup chave cript].**

7. **Especifique como realizar o backup da chave de criptografia.**

   Caso tenha selecionado [Salvar no SD], insira um cartão SD no slot de mídia na parte lateral do painel de controle e pressione [OK]. Após o backup da chave de criptografia de dados do equipamento, pressione [Sair].

   Para obter informações sobre como manusear e inserir o cartão SD, consulte Getting Started.

   Se você selecionou a opção [Imprimir em pap], pressione a tecla [Iniciar] e imprima a chave de criptografia de dados do equipamento.

8. **Pressione [Sair].**
9. **Faça logout.**

4

Atualizar a chave de criptografia

Você pode atualizar a chave de criptografia. A aplicação da nova chave de criptografia levará o mesmo tempo do procedimento de inicialização da criptografia. As atualizações podem ser feitas quando o equipamento estiver funcionando normalmente.

Importante

- O equipamento não pode ser utilizado enquanto a chave de criptografia está sendo atualizada.
- A chave de criptografia é necessária para recuperação se o equipamento apresentar defeito. Certifique-se de armazenar a chave de criptografia de modo seguro para a recuperação de dados de backup.
- Quando a chave de criptografia é atualizada, a criptografia é efetuada utilizando a nova chave. Após a conclusão do procedimento no painel de controle de equipamento, desligue a alimentação principal e reinicie o equipamento para habilitar as novas definições. A reinicialização pode ser lenta se houver dados a serem transferidos para o disco rígido.
- Depois que a atualização da chave de criptografia é iniciada, ela não pode ser parada. Certifique-se de que o equipamento não seja desligado durante o processo de criptografia. Se o equipamento for desligado durante a criptografia, o disco rígido será danificado e os dados contidos nele ficarão inutilizados.
- Se a atualização da chave de criptografia não for concluída, a chave de criptografia criada não será válida.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Definições de criptografia de dados da máquina].**

6. **Pressione [Atualiz chave de cript].**

7. **Selecione os dados que serão transferidos para o disco rígido e o que não deve ser excluído.**

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Som dados sist de arq]. Para excluir todos os dados, selecione [Formatar todos os dados].

8. **Especifique como realizar o backup da chave de criptografia.**

   Caso tenha selecionado [Save to SD Card] (Salvar no cartão SD), insira um cartão SD no slot de mídia na parte lateral do painel de controle e pressione [OK] para fazer o backup da chave de criptografia de dados da máquina.

   Para obter informações sobre como manusear e inserir o cartão SD, consulte Getting Started.

   Se você selecionou a opção [Imprimir em pap], pressione a tecla [Iniciar] e imprima a chave de criptografia de dados do equipamento.

9. **Pressione [OK].**
10. **Pressione [Sair].**
11. **Pressione [Sair].**
12. **Faça logout.**
13. **Desligue o equipamento e, em seguida, religue-o novamente.**

   O equipamento começará a converter os dados na memória depois que você ligá-lo. Aguarde até que a mensagem "Conversão de memória concluída. Desligue a chave de energia principal." seja exibida, em seguida desligue a chave de energia principal novamente.

   Para obter informações sobre como desligar a alimentação principal, consulte Getting Started.

Cancelar a criptografia de dados

Efetue o procedimento a seguir para cancelar as definições de criptografia quando a criptografia não for mais necessária. A ativação e desativação das definições de criptografia demoram o mesmo tempo.

Importante

- Não é possível utilizar o equipamento durante o cancelamento da criptografia de dados.
- Depois de fazer este procedimento no painel de controle do equipamento, desligue a energia principal do equipamento e reinicie-o para ativar as novas definições. A reinicialização pode ser lenta se houver dados a serem transferidos para o disco rígido.
- Depois que o cancelamento de criptografia dos dados iniciar, ele não pode ser parado. Certifique-se de que o equipamento não seja desligado durante o processo de criptografia. Se o equipamento for desligado durante a criptografia, o disco rígido será danificado e os dados contidos nele ficarão inutilizados.
- Antes de descartar um equipamento, apague completamente a memória. Para obter detalhes sobre como apagar toda a memória, consulte Pág. 97 "Excluir dados no equipamento".

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Definições de criptografia de dados da máquina].**
6. **Pressione [Cancelar criptografia].**
7. **Selecione os dados que serão transferidos para o disco rígido e o que não deve ser excluído.**

   Para transferir todos os dados para o disco rígido, selecione [Todos os dados]. Para transferir apenas os dados das definições do equipamento, selecione [Som dados sist de arq]. Para excluir todos os dados, selecione [Formatar todos os dados].
8. **Pressione [OK].**
9. **Pressione [Sair].**
10. **Pressione [Sair].**
11. **Faça logout.**
12. **Desligue o equipamento e, em seguida, religue-o novamente.**

    Para obter informações sobre como desligar a alimentação principal, consulte Getting Started.

Excluir dados no equipamento

É possível evitar a perda de dados sobrescrevendo os dados armazenados no equipamento.

Existem dois tipos de sobrescrição:

Apagamento automático da memória

Os dados temporariamente armazenados no disco rígido do equipamento para copiar ou imprimir são automaticamente apagados. Para mais informações, consulte Pág. 97 "Apagar automaticamente a memória".

Apagar toda a memória

Todos os dados armazenados no disco rígido da máquina são apagados com a sobrescrição. As definições do dispositivo armazenadas na memória do equipamento são inicializadas. Execute esse procedimento para apagar todos os dados e definições ao mudar a localização ou descartar o equipamento. Para mais informações, consulte Pág. 102 "Apagar toda a memória".

Apagar automaticamente a memória

Um documento digitalizado no modo copiadora ou scanner ou os dados de impressão enviados a partir de um driver de impressão são temporariamente armazenados no disco rígido do equipamento. Mesmo após a conclusão do trabalho, eles permanecem no disco rígido como dados temporários. A função Apagar automaticamente a memória apaga os dados temporários no disco rígido, substituindo--os.

A substituição começa automaticamente assim que o trabalho terminar.

As funções de copiadora e impressora têm prioridade sobre a função Apagar automaticamente a memória. Se um trabalho de cópia ou impressão estiver em andamento, a substituição dos dados será realizada apenas depois da conclusão do trabalho.

Tipos de dados que podem ou não ser substituídos pelo apagamento automático da memória

Dados substituídos pela função Apagar automaticamente a memória

Copiadora

- Trabalhos de cópia

Impressora

- Trabalhos de impressão
- Trabalhos de Impressão de teste/Impressão bloqueada/Reter impressão/Impressão armazenada

Um trabalho de Impressão de teste/Impressão bloqueada/Reter impressão só pode ser substituído depois de executado. Um trabalho de Impressão armazenada é substituído depois de ser excluído.

- Trabalhos de impressão em spool

Scanner

- Arquivos digitalizados enviados por e-mail
- Arquivos enviados por Scan to Folder
- Documentos enviados utilizando o Web Image Monitor
- Scanner TWAIN de rede

  Os dados digitalizados com o scanner TWAIN de rede quando a função "ADF(Leitura antecipada)" do driver TWAIN estiver selecionada serão substituídos pela definição Apagar automaticamente a memória.

  Os dados digitalizados quando a função "ADF(Leitura antecipada)" não estiver selecionada não serão substituídos.

Servidor de documentos

- Documentos armazenados pelo usuário no Servidor de documentos utilizando as funções de copiadora, impressora ou scanner

  Um documento armazenado só pode ser substituído depois de ser impresso ou excluído do Servidor de documentos.

Outro

- Informações registradas no Catálogo de endereços

  Os dados armazenados no Catálogo de endereços só podem ser substituídos após terem sido alterados ou excluídos.

- Aplicativos utilizando Embedded Software Architecture

  Os dados do programa Embedded Software Architecture só podem ser substituídos após terem sido excluídos.

Dados não substituídos por Apagar automaticamente a memória

- Contadores em cada código de usuário

Métodos de substituição

Você pode selecionar um dos seguintes métodos de substituição:

- NSA

  Os dados temporários são substituídos duas vezes por números aleatórios e uma vez por zeros.

- DoD

Cada item dos dados é substituído por um número aleatório, depois pelo seu complemento, depois por outro número aleatório e é, então, verificado.

- Números aleatórios

  Os dados temporários são substituídos várias vezes por números aleatórios. O número de substituições pode ser selecionado de 1 a 9.

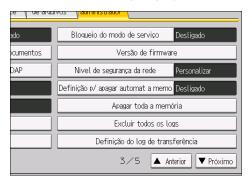
- O método padrão de substituição é "Números aleatórios", e o número padrão de substituições é 3.
- NSA significa "National Security Agency", EUA
- DoD significa "Department of Defense", EUA.

Utilizar Apagar automaticamente a memória

Importante

- Quando Apagar automaticamente a memória está definido como [Ligado], os dados temporários que ficaram no disco rígido quando Apagar automaticamente a memória [Desligado] podem não ser substituídos.
- Se o botão liga/desliga estiver na posição de desligado antes da conclusão da operação Apagar automaticamente a memória, a substituição será interrompida e os dados permanecerão no disco rígido.
- Não interrompa o processo de substituição. Caso contrário, o disco rígido pode ser danificado.
- Se o botão de alimentação principal for colocado na posição de desligado antes da conclusão da operação Apagar automaticamente a memória, a substituição continuará assim que o botão de alimentação principal for colocado novamente na posição de ligado.
- Se ocorrer um erro antes da conclusão da substituição, desligue o equipamento. Ligue-o e, em seguida, repita a partir da etapa 1.
- O equipamento não entrará no modo Suspensão até que a substituição tenha sido concluída.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**

5. **Pressione [Definição p/ apagar automat a memo].**

6. **Pressione [Ligado].**
7. **Selecione o método de substituição que pretende utilizar.**

   Se você selecionar [NSA] ou [DoD], avance para a etapa 10.

   Se você selecionar [Números aleatórios], avance para a etapa 8.
8. **Pressione [Alterar].**
9. **Insira o número de vezes que deseja substituir utilizando as teclas numéricas e pressione [#].**
10. **Pressione [OK].**

    A opção Apagar automaticamente a memória é definida.
11. **Faça logout.**

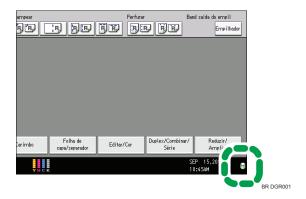
- Se ativar a substituição e a criptografia dos dados, os dados de substituição também serão criptografados.

Cancelar a função Apagar automaticamente a memória

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**
5. **Pressione [Definição p/ apagar automat a memo].**
6. **Pressione [Desligado].**
7. **Pressione [OK].**

   A opção Apagar automaticamente a memória é desativada.
8. **Faça logout.**

Ícone Substituir

Quando a opção para apagar automaticamente a memória estiver habilitada, o ícone Substituir dados será indicado no canto inferior direito do painel do equipamento.

Ícone	Nome do ícone	Explicação
	Com dados	Este ícone acende quando existem dados temporários a ser substituídos e pisca durante a substituição.
	Limpar	Este ícone acende quando não existem dados temporários a serem substituídos.

Importante

- **O ícone Substituir dados indicará "Sem dados" quando houver um trabalho de impressão de teste/impressão bloqueada/reter impressão/impressão armazenada.**

- Se o ícone Substituir Dados não for exibido, verifique primeiro se Apagar automaticamente a memória está definido como [Desligado]. Se o ícone não for exibido mesmo que Apagar automaticamente a memória esteja [Ligado], contate seu representante técnico.
- Se o equipamento entrar no modo de economia de energia durante a substituição, pressione a tecla [Economia de energia] para reativar o visor e verificar o ícone.
- Se o ícone Substituir dados continuar "Sujo" sem a presença de dados para substituição, desligue a alimentação do equipamento. Ligue-o novamente e veja se o ícone muda para "Sem dados". Se não mudar, contate o seu representante de vendas ou técnico.

Apagar toda a memória

Substitua e apague todos os dados armazenados no disco rígido quando mudar a localização ou descartar o equipamento. As definições do dispositivo armazenadas na memória do equipamento são inicializadas.

Para obter detalhes sobre como utilizar o equipamento depois de executar Apagar toda a memória, entre em contato com o representante de vendas.

Importante

- Se o botão liga/desliga estiver na posição de desligado antes da conclusão da função "Apagar toda a memória", a substituição será interrompida e os dados permanecerão no disco rígido.
- Não interrompa o processo de substituição. Caso contrário, o disco rígido pode ser danificado.
- Recomenda-se que, antes de apagar o disco rígido, você use o Device Manager NX para fazer backup do Catálogo de endereços. Também é possível fazer backup do Catálogo de endereços utilizando o Web Image Monitor. Para obter informações, consulte a Ajuda do Device Manager NX ou a Ajuda do Web Image Monitor.
- A única operação possível durante o processo "Apagar toda a memória" é pausar. Se for selecionado "Números aleatórios" e sobrescrever for igual a três vezes, o processo "Apagar toda a memória" levará até 5 horas e 15 minutos.
- A função "Apagar toda a memória" também apaga todas as definições de segurança do equipamento, deixando inoperante a administração do equipamento e dos usuários. Certifique-se de que os usuários não armazenem nenhum dado no equipamento após a conclusão de "Apagar toda a memória".

Tipos de dados que podem ser substituídos por Apagar toda a memória

Copiadora

- Trabalhos de cópia

Impressora

- Trabalhos de impressão
- Trabalhos de Impressão de teste/Impressão bloqueada/Reter impressão/Impressão armazenada
- Trabalhos de impressão em spool

Scanner

- Arquivos digitalizados enviados por e-mail
- Arquivos enviados por Scan to Folder
- Documentos enviados utilizando o Web Image Monitor
- Scanner TWAIN de rede

Os dados digitalizados com o scanner TWAIN de rede quando a função "ADF(Leitura antecipada)" do driver TWAIN estiver selecionada serão substituídos pela definição Apagar automaticamente a memória.

Os dados digitalizados quando a função "ADF(Leitura antecipada)" não estiver selecionada não serão substituídos.

Servidor de documentos

- Documentos armazenados pelo usuário no Servidor de documentos utilizando as funções de copiadora, impressora ou scanner

Outro

- Informações registradas no Catálogo de endereços
- Contadores em cada código de usuário
- Aplicativos utilizando Arquitetura de Software Incorporada

Definições do sistema ou outras definições relacionadas ao dispositivo são inicializadas.

Métodos para apagar

Você pode selecionar um dos seguintes métodos de apagar:

- NSA

  Os dados são substituídos duas vezes por números aleatórios e uma vez por zeros.
- DoD

  Os dados são substituídos por um número aleatório, depois pelo seu complemento, depois por outro número aleatório e, então, verificado.
- Números aleatórios

  Os dados são substituídos várias vezes por números aleatórios. O número de substituições pode ser selecionado de 1 a 9.
- BSI/VSITR

  Os dados são substituídos 7 vezes pelos seguintes padrões: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.
- Apagar com segurança

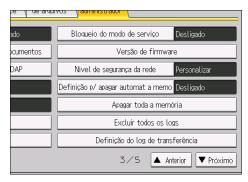
  Os dados são substituídos por um algoritmo criado no drive do disco rígido.
- Formato

  O disco rígido está formatado. Os dados não foram substituídos.

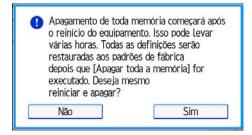
- O método padrão para apagar é "Números aleatórios", e o número padrão de substituições é 3.

- NSA significa "National Security Agency", EUA
- DoD significa "Department of Defense", EUA.

Utilizar Apagar toda a memória

1. **Desconecte os cabos de comunicação do equipamento.**
2. **Faça login como administrador do equipamento no painel de controle.**
3. **Pressione [Definições do sistema].**
4. **Pressione [Ferramentas admin].**
5. **Pressione [▼Próximo] duas vezes.**
6. **Pressione [Apagar toda a memória].**

7. **Selecione o método de apagar.**

   Se selecionar [NSA], [DoD], [BSI/VSITR], [Apagar com segurança], ou [Formatar], vá para a Etapa 10.

   Se você selecionar [Números aleatórios], avance para a etapa 8.
8. **Pressione [Alterar].**
9. **Insira o número de vezes que deseja substituir utilizando as teclas numéricas e pressione [#].**
10. **Pressione [Apagar].**
11. **Pressione [Sim].**

12. Após terminar de apagar, pressione [Sair] e desligue o equipamento.

Para obter informações sobre como desligar a alimentação principal, consulte Getting Started.

- Se o botão de alimentação principal for colocado na posição de desligado antes da conclusão da função "Apagar toda a memória", a substituição iniciará novamente assim que o botão de alimentação principal for colocado novamente na posição de ligado.
- Se ocorrer um erro antes da conclusão da substituição, desligue o equipamento. Ligue-o novamente e repita a partir da etapa 2.

Suspender a função Apagar toda a memória

Para desligar a energia do equipamento enquanto Apagar toda a memória estiver habilitado, suspenda Apagar toda a memória previamente. Apagar toda a memória continuará quando você ligar a energia principal.

- Se [Apagar com segurança] ou [Formatar] estiver selecionado, o processo não poderá ser suspenso.
- Apagar toda a memória não pode ser cancelado.

1. Pressione [Parar] enquanto Apagar toda a memória estiver em andamento.

2. Pressione [Sim].

Apagar toda a memória é suspenso.

3. Desligue o equipamento.

Para obter informações sobre como desligar a alimentação principal, consulte Getting Started.

5. Segurança de rede avançada

Este capítulo descreve as funções que aumentam a segurança do equipamento quando ele está conectado à rede.

Controle de acesso

O equipamento pode controlar o acesso por TCP/IP.

Limite os endereços IP a partir dos quais o acesso é possível especificando um intervalo do controle de acesso.

Por exemplo, se você especificar um intervalo do controle de acesso como [192.168.15.16]-[192.168.15.20], os endereços do PC cliente a partir dos quais o acesso é possível serão de [192.168.15.16] a [192.168.15.20].

Importante

- Usando o controle de acesso, é possível limitar os acessos de LPR, RCP/RSH, FTP, ssh/sftp, Bonjour, SMB, WSD (dispositivo), WSD (impressora), WSD (scanner)/DSM, IPP, DIPRINT, RHPP ou Web Image Monitor. Não é possível limitar acessos a partir do telnet ou Device Manager NX ao usar SNMPv1 para monitoramento.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Controle de acesso] no menu "Segurança".**
4. **Para especificar o endereço IPv4, insira um endereço IP com acesso ao equipamento em "Intervalo de controle de acesso".**

   Para especificar o endereço IPv6, insira um endereço IP que tenha acesso ao equipamento em "Intervalo" em "Intervalo de controle de acesso" ou insira um endereço IP em "Máscara" e especifique o "Comprimento da máscara".
5. **Clique em [OK].**
6. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

Ativar e desativar protocolos

Especifique se deseja ativar ou desativar a função para cada protocolo. Ao efetuar esta definição, você pode especificar que protocolos estão disponíveis, prevenindo assim o acesso não autorizado pela rede. As definições de rede podem ser especificadas no painel de controle ou utilizando o Web Image Monitor, telnet, Device Manager NX ou Remote Communication Gate S.

Protocolo	Porta	Método de definição	Quando desativado
IPv4	-	• Painel de controle • Web Image Monitor • telnet	Nenhum aplicativo que opere através de IPv4 pode ser utilizado. Não é possível desativar o IPv4 no Web Image Monitor durante uma transmissão IPv4.
IPv6	-	• Painel de controle • Web Image Monitor • telnet	Todos os aplicativos que operam através de IPv6 não podem ser utilizados.
IPsec	-	• Painel de controle • Web Image Monitor • telnet	A transmissão criptografada utilizando IPsec é desativada.
FTP	TCP:21	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem FTP não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controle utilizando "Restringir visualiz de destinos de usuários".
ssh/sftp	TCP:22	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem sftp não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controle utilizando "Restringir visualiz de destinos de usuários".
telnet	TCP:23	• Web Image Monitor • Device Manager NX	Comandos que utilizam telnet são desativados.

Protocolo	Porta	Método de definição	Quando desativado
SMTP	TCP:25 (variável)	• Painel de controle • Web Image Monitor • Device Manager NX • Remote Communication Gate S	Não é possível utilizar as funções de notificação por e-mail que requerem recepção SMTP.
HTTP	TCP:80	• Web Image Monitor • telnet	As funções que requerem HTTP não podem ser utilizadas. Não é possível imprimir utilizando IPP na porta 80.
HTTPS	TCP:443	• Web Image Monitor • telnet	As funções que requerem HTTPS não podem ser utilizadas. Não é possível utilizar o @Remote. Você também pode efetuar definições para exigir transmissão SSL utilizando o painel de controle ou o Web Image Monitor.
SMB	TCP:139	• Painel de controle • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções de impressão SMB não podem ser utilizadas.
NBT	UDP:137 UDP:138	• telnet	As funções de impressão SMB via TCP/IP e as funções designadas NetBIOS no servidor WINS não podem ser utilizadas.
SNMPv1,v2	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem SNMPv1, v2 não podem ser utilizadas. Utilizando o painel de controle, Web Image Monitor ou telnet, você pode especificar as definições SNMPv1, v2 como somente leitura, não podendo ser editadas.

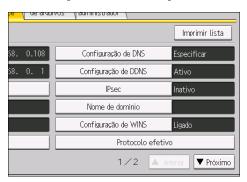
Protocolo	Porta	Método de definição	Quando desativado
SNMPv3	UDP:161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que requerem SNMPv3 não podem ser utilizadas. Você também pode especificar as definições para exigir transmissão criptografada SNMPv3 e restringir a utilização de outros métodos de transmissão usando o painel de controle, Web Image Monitor ou telnet.
RSH/RCP	TCP:514	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	As funções que exigem RSH e as funções da rede TWAIN não podem ser utilizadas. É possível restringir a visualização de informações pessoais efetuando definições no painel de controle utilizando "Restringir visualiz de destinos de usuários".
LPR	TCP:515	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções LPR. É possível restringir a visualização de informações pessoais efetuando definições no painel de controle utilizando "Restringir visualiz de destinos de usuários".
IPP	TCP:631	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções IPP.
SSDP	UDP:1900	• Web Image Monitor • telnet	A localização de dispositivos utilizando UPnP a partir do Windows não pode ser utilizada.
Bonjour	UDP:5353	• Web Image Monitor • telnet	Não é possível utilizar funções Bonjour.

Protocolo	Porta	Método de definição	Quando desativado
@Remote	TCP:7443 TCP:7444	• Painel de controle • telnet	Não é possível utilizar o @Remote.
DIPRINT	TCP:9100	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível utilizar funções DIPRINT.
RFU	TCP:10021	• Painel de controle • telnet	É possível atualizar o firmware via FTP.
NetWare	(IPX/SPX)	• Painel de controle • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	Não é possível imprimir com NetWare. Não é possível utilizar SNMP via IPX.
WSD (Dispositivo)	TCP:53000 (variável)	• Web Image Monitor • telnet	Não é possível utilizar funções WSD (Dispositivo).
WSD (Impressora)	TCP:53001 (variável)	• Web Image Monitor • telnet	Não é possível utilizar funções WSD (Impressora).
WSD (Scanner)/DSM	TCP-53002 (variável)	• Web Image Monitor • telnet	WSD (Scanner) e funções DSM não podem ser usados.
WS-Discovery	UDP/TCP: 3702	• telnet	Não é possível utilizar a função de pesquisa WSD (Dispositivo, Impressora, Scanner).
RHPP	TCP:59100	• Web Image Monitor • telnet	Não é possível imprimir com RHPP.
LLTD	-	• telnet	A função de pesquisa de dispositivos utilizando LLTD não pode ser usada.

Protocolo	Porta	Método de definição	Quando desativado
LLMNR	UDP:5355	• Web Image Monitor • telnet	As solicitações de resolução de nome utilizando LLMNR não podem ser respondidas.

- "Restringir visualiz de destinos de usuários" é um dos recursos da Segurança estendida. Para obter mais informações sobre como efetuar esta definição, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

Ativar e desativar protocolos utilizando o painel de Controle

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Definições de interface].**
4. **Pressione [Protocolo efetivo].**

5. **Selecione o protocolo que deseja ativar ou desativar.**

6. **Pressione [OK].**
7. **Faça logout.**

Ativar e desativar protocolos utilizando o Web Image Monitor

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Segurança da rede] em "Segurança".**
4. **Selecione o protocolo que deseja ativar ou desativar, ou selecione a porta que deseja abrir ou fechar.**
5. **Clique em [OK].**
6. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

Especificar Níveis de segurança da rede

Esta definição permite alterar os níveis de segurança para limitar o acesso não autorizado. É possível configurar as definições do nível de segurança da rede utilizando o painel de controle ou Web Image Monitor. Observe que os protocolos que podem ser especificados variam.

Importante

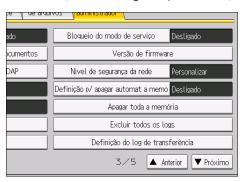
- Quando algumas utilitários, a comunicação ou o login podem falhar dependendo do nível de segurança da rede.

Níveis de segurança da rede

Nível de segurança	Descrição
[Nível 0]	Selecione [Nível 0] para utilizar todas as funções. Utilize esta definição se não tiver informações que precisem ser protegidas contra ameaças externas.
[Nível 1]	Selecione [Nível 1] para segurança moderada e proteção de informações importantes. Utilize esta definição se o equipamento estiver conectado a uma rede local (LAN).
[FIPS140]	Oferece um grau de segurança intermediário entre [Nível 1] e [Nível 2]. Só é possível usar códigos recomendados pelo governo dos EUA como algoritmo de codificação/autenticação. As definições diferentes do algoritmo são as mesmas que as do [Nível 2].
[Nível 2]	Selecione [Nível 2] para segurança máxima e proteção de informações confidenciais. Utilize esta definição quando for necessário proteger informações contra ameaças externas.
[Personalizar]	Para outras configurações diferentes dos níveis acima. Configure usando o Web Image Monitor.

Especificar os níveis de segurança da rede utilizando o painel de controle

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**

5. **Pressione [Nível de segurança da rede].**

6. **Selecione o nível desejado de segurança da rede.**

   Selecione [Nível 0], [Nível 1], [Nível 2], ou [FIPS140].

7. **Pressione [OK].**
8. **Faça logout.**

Especificar o nível de segurança da rede utilizando o Web Image Monitor

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Segurança da rede] em "Segurança".**
4. **Selecione o nível de segurança da rede em "Nível de segurança".**
5. **Clique em [OK].**
6. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.

7. **Faça logout.**

Status das funções em cada nível de segurança da rede

TCP/IP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
TCP/IP	Ativo	Ativo	Ativo	Ativo
HTTP > Porta 80	Aberto	Aberto	Aberto	Aberto

Função	Nível 0	Nível 1	FIPS 140	Nível 2
IPP> Porta 80	Aberto	Aberto	Aberto	Aberto
IPP> Porta 631	Aberto	Aberto	Fechar	Fechar
SSL/TLS> Porta 443	Aberto	Aberto	Aberto	Aberto
SSL/TLS> Permitir comunicação SSL/TLS	Prioridade de texto cifrado	Prioridade de texto cifrado	Somente texto cifrado	Somente texto cifrado
Versão do SSL/TLS > TLS1.2	Ativo	Ativo	Ativo	Ativo
Versão do SSL/TLS > TLS1.1	Ativo	Ativo	Ativo	Ativo
Versão do SSL/TLS > TLS1.0	Ativo	Ativo	Ativo	Ativo
Versão do SSL/TLS > SSL3.0	Ativo	Ativo	Inativo	Inativo
Definição do grau de criptografia> AES	128bits/ 256bits	128bits/ 256bits	128bits/ 256bits	128bits/ 256bits
Definição do grau de criptografia> 3DES	168bits	168bits	168bits	-
Definição do grau de criptografia>RC4	-	-	-	-
DIPRINT	Ativo	Ativo	Inativo	Inativo
LPR	Ativo	Ativo	Inativo	Inativo
FTP	Ativo	Ativo	Ativo	Ativo
sftp	Ativo	Ativo	Ativo	Ativo
ssh	Ativo	Ativo	Ativo	Ativo
RSH/RCP	Ativo	Ativo	Inativo	Inativo
TELNET	Ativo	Inativo	Inativo	Inativo
Bonjour	Ativo	Ativo	Inativo	Inativo
SSDP	Ativo	Ativo	Inativo	Inativo
SMB	Ativo	Ativo	Inativo	Inativo
NetBIOS sobre TCP/IPv4	Ativo	Ativo	Inativo	Inativo

Função	Nível 0	Nível 1	FIPS 140	Nível 2
WSD (Device)	Ativo	Ativo	Ativo	Ativo
WSD (Printer)	Ativo	Ativo	Ativo	Ativo
WSD (Scanner)/DSM	Ativo	Ativo	Ativo	Ativo
WSD (Comunicação criptografa de dispositivo)	Inativo	Inativo	Ativo	Ativo
RHPP	Ativo	Ativo	Inativo	Inativo

As mesmas definições aplicam-se a IPv4 e IPv6.

A definição TCP/IP não é controlada pelo nível de segurança. Especifique manualmente a ativação ou desativação desta definição.

NetWare

Função	Nível 0	Nível 1	FIPS 140	Nível 2
NetWare	Ativo	Ativo	Inativo	Inativo

Se o Netware não for utilizado na sua rede, as definições acima não se aplicam.

SNMP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
SNMP	Ativo	Ativo	Ativo	Ativo
Permitir definições por SNMPv1 e v2	Ligado	Desligado	Desligado	Desligado
Função SNMPv1,v2	Ativo	Ativo	Inativo	Inativo
Função SNMPv3	Ativo	Ativo	Ativo	Ativo
Permitir comunicação SNMPv3	Criptografia /Texto não criptografado	Criptografia /Texto não criptografado	Somente criptografia	Somente criptografia

Definição do grau de criptografia TCP/IP

Função	Nível 0	Nível 1	FIPS 140	Nível 2
ssh > Algoritmo de criptografia	DES/3DES/AES-128/AES-192/AES-256/Blowfish/Arcfour	3DES/AES-128/AES-192/AES-256/Arcfour	3DES/AES-128/AES-192/AES-256	3DES/AES-128/AES-192/AES-256
S/MIME > Algoritmo de criptografia	3DES-168 bits	3DES-168 bits	3DES-168 bits	AES-256 bits
S/MIME > Algoritmo digest	SHA1	SHA1	SHA1	SHA-256 bits
SNMPv3 > Algoritmo de autenticação	MD5	SHA1	SHA1	SHA1
SNMPv3 > Algoritmo de criptografia	DES	DES	AES-128	AES-128
Autenticação Kerberos > Algoritmo de criptografia	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC/DES-CBC-MD5	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96
Chave de criptografia de driver > Grau de criptografia	Criptografia simples	DES	AES	AES

Proteger os caminhos de comunicação via certificado de dispositivo

Este equipamento pode proteger os caminhos de comunicação e estabelecer comunicações criptografadas utilizando SSL/TLS, IPsec, S/MIME ou IEEE 802.1X. Também pode proteger PDFs utilizando uma assinatura digital de PDF ou PDF/A

Para usar essas funções, é necessário primeiro criar e instalar um certificado de dispositivo para o equipamento.

Os seguintes tipos de certificado de dispositivo podem ser usados:

- Certificado autoassinado pela máquina
- Certificado emitido por uma autoridade de certificado

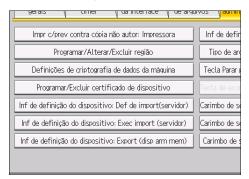
- **O administrador deve gerenciar a expiração dos certificados e renová-los antes de expirarem.**
- **O administrador deve assegurar que o emissor do certificado seja uma autoridade competente.**

5

Criar e instalar um certificado de dispositivo via painel de controle (certificado autoassinado)

Criar e instalar o certificado de dispositivo usando o painel de controle.

Este capítulo explica a utilização de um certificado autoassinado como o certificado de dispositivo.

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Programar/Excluir certificado de dispositivo].**

6. **Certifique-se de que [Programar] esteja selecionado.**

7. **Pressione [Certificado 1].**

    Somente o [Certificado 1] pode ser criado via painel de controle.

8. **Configure as definições necessárias.**

    Para usar o certificado do dispositivo para S/MIME, Assinatura digital de PDF ou Assinatura digital de PDF/A, insira o e-mail do administrador do equipamento na definição de endereço de e-mail.

9. **Pressione [OK].**

    "Instalado" é exibido em "Status do certificado" para mostrar que o certificado de dispositivo da máquina foi instalado.

10. **Faça logout.**

- Selecione [Excluir] para excluir o certificado de dispositivo do equipamento.
- Para usar o certificado de dispositivo criado no equipamento para S/MIME ou Assinatura digital de PDF/A, defina "Certificação" em Web Image Monitor como [Certificado 1].

Criar e instalar um certificado de dispositivo a partir do Web Image Monitor (Certificado autoassinado)

Crie e instale o certificado de dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens exibidos e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado autoassinado como o certificado de dispositivo.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o botão de opção ao lado do número do certificado que deseja criar.**

    Para usar SSL/TLS, selecione [Certificado 1]. Para usar outro protocolo, selecione o número do certificado a ser usado.

5. **Clique em [Criar].**

    Clique em [Excluir] para excluir o certificado de dispositivo do equipamento.

6. **Configure as definições necessárias.**

    Para usar o certificado do dispositivo para S/MIME, Assinatura digital de PDF ou Assinatura digital de PDF/A, insira o e-mail do administrador do equipamento na definição de endereço de e-mail.

7. **Clique em [OK].**

    A definição é alterada.

8. **Clique em [OK].**
9. **Se aparecer uma mensagem de aviso, verifique os detalhes e selecione "Continuar neste site".**

   "Instalado" é exibido em "Status do certificado" para mostrar que o certificado de dispositivo da máquina foi instalado.
10. **Faça logout.**

Criar um certificado de dispositivo (emitido por uma autoridade de certificação)

Crie o certificado de dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens exibidos e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado emitido por uma autoridade de certificação como certificado de dispositivo.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o botão de opção ao lado do número do certificado que deseja criar.**

   Para usar SSL/TLS, selecione [Certificado 1]. Para usar outro protocolo, selecione o número do certificado a ser usado.
5. **Clique em [Solicitar].**
6. **Configure as definições necessárias.**
7. **Clique em [OK].**

   A definição é alterada.
8. **Clique em [OK].**

   "Solicitando" é exibido para "Status do certificado".
9. **Faça logout.**
10. **Solicite um certificado de dispositivo à autoridade de certificação.**

    O processo do pedido depende da autoridade de certificação. Para mais informações, contate a autoridade de certificação.

    Para fazer o pedido, clique no ícone Web Image Monitor Detalhes e use as informações mostradas em "Detalhes do certificado".

- Se você pedir 2 certificados ao mesmo tempo, o local da emissão pode não ser exibido. Quando você instala um certificado, não se esqueça de verificar o destino e o processo de instalação do certificado.
- O Web Image Monitor pode ser utilizado para criar o certificado do dispositivo, mas não para solicitar o certificado à autoridade de certificação.
- Clique em [Cancelar solicitação] para cancelar a solicitação de certificado de dispositivo.

Instalar um certificado de dispositivo (emitido por uma autoridade de certificação)

Instale o certificado de dispositivo utilizando o Web Image Monitor. Para mais informações sobre os itens exibidos e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.

Este capítulo explica a utilização de um certificado emitido por uma autoridade de certificação como certificado de dispositivo.

Insira o conteúdo do certificado de dispositivo emitido pela autoridade de certificação.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o botão de opção ao lado do número de certificado que deseja instalar.**

   Para usar SSL/TLS, selecione [Certificado 1]. Para usar outro protocolo, selecione o número do certificado a ser usado.
5. **Clique em [Install].**
6. **Insira o conteúdo do certificado do dispositivo.**

   Na caixa de certificação, introduza o conteúdo do certificado do dispositivo emitido pela autoridade de certificação.

   Se estiver instalando um certificado intermediário, insira também o conteúdo do certificado intermediário.

   Para mais informações sobre os itens exibidos e os que podem ser selecionados, consulte a Ajuda do Web Image Monitor.
7. **Clique em [OK].**
8. **Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   "Instalado" é exibido em "Status do certificado" para mostrar que o certificado de dispositivo da máquina foi instalado.

9. **Faça logout.**

Instalar um certificado intermediário (emitido por uma autoridade de certificação)

Esta seção explica como utilizar o Web Image Monitor para instalar um certificado intermediário emitido por uma autoridade de certificação.

Se você não tiver o certificado intermediário emitido pela autoridade de certificação, aparecerá uma mensagem de aviso durante a comunicação. Se a autoridade de certificação emitiu um certificado intermediário, recomendamos que você instale-o.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o botão de opção ao lado do número de certificado que deseja instalar.**
5. **Clique em [Instalar certificado intermediário].**
6. **Insira o conteúdo do certificado intermediário.**

   Na caixa de certificação, insira o conteúdo do certificado intermediário emitido pela autoridade de certificação. Para obter detalhes sobre os itens e definições de um certificado, consulte a Ajuda do Web Image Monitor.

7. **Clique em [OK].**
8. **Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   O certificado intermediário será instalado no dispositivo. A tela "Detalhes do certificado" indica se o certificado intermediário foi instalado ou não. Para mais informações sobre a tela "Detalhes do certificado", consulte a Ajuda do Web Image Monitor.

9. **Faça logout.**

Configurar definições SSL/TLS

Quando o equipamento é configurado para usar SSL/TLS, a comunicação criptografada é ativada. Isso ajuda a evitar que os dados sejam interceptados, craqueados ou violados durante a transmissão.

Fluxo de comunicações criptografadas SSL/TLS

1. Para acessar o equipamento a partir do computador de um usuário, solicite o certificado de dispositivo SSL/TLS e uma chave pública.

2. O certificado de dispositivo e a chave pública são enviados do equipamento para o computador do usuário.

3. A chave compartilhada criada com o computador é criptografada usando a chave pública, enviada para a máquina e descriptografada usando a chave privada no equipamento.

4. A chave compartilhada é usada para criptografia e descriptografia de dados, proporcionando, assim, uma transmissão segura.

Fluxo de configuração ao usar um certificado de autoassinatura

1. Criar e instalar o certificado de dispositivo:

Crie e instale um certificado de dispositivo usando o painel de controle ou o Web Image Monitor.

2. Ativar SSL/TLS:

   Ative a definição SSL/TLS usando o Web Image Monitor.

Fluxo de configuração ao usar um certificado emitido por uma autoridade

1. Criar um certificado de dispositivo e aplicar à autoridade:

   Depois de criar um certificado de dispositivo no Web Image Monitor, aplique-o à autoridade de certificação.

   O procedimento do pedido após a criação do certificado depende da autoridade de certificação. Siga o procedimento especificado pela autoridade de certificação.

2. Instalar o certificado de dispositivo:

   Instale o certificado de dispositivo utilizando o Web Image Monitor.

3. Ativar SSL/TLS:

   Ative a definição SSL/TLS usando o Web Image Monitor.

- Para verificar se a configuração SSL/TLS está ativa, insira "https://(endereço IP ou nome de host do equipamento)/" na barra de endereços do navegador da Web para acessar este equipamento. Se aparecer a mensagem "A página não pode ser exibida", verifique a configuração, pois a configuração SSL/TLS atual não é válida.
- Se você ativar SSL/TLS para IPP (funções de impressora), os dados enviados serão criptografados, evitando que sejam interceptados, analisados ou manipulados.

Ativar SSL/TLS

Depois de instalar o certificado de dispositivo no equipamento, ative a definição SSL/TLS.

Este procedimento é utilizado para um certificado autoassinado ou para um certificado emitido por uma autoridade de certificação.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [SSL/TLS] em "Segurança".**
4. **Para IPv4 e IPv6, selecione "Ativo" se desejar ativar SSL/TLS.**
5. **Selecione o modo de comunicação de criptografia para "Permitir comunicação SSL/TLS".**
6. **Se você desejar desativar um protocolo, clique em [Inativo] próximo a "TLS1.2", "TLS1.1", "TLS1.0" ou "SSL3.0".**

   Pelo menos um desses protocolos deve estar ativado.

7. **Em "Definição do grau de criptografia", especifique o grau de criptografia a ser aplicado: "AES", "3DES", e/ou "RC4". Você deve marcar, pelo menos, uma caixa de seleção.**

   Observe que a disponibilidade de graus de criptografia variam dependendo das definições especificadas para "TLS1.2", "TLS1.1", "TLS1.0" ou "SSL3.0".

8. **Clique em [OK].**

9. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.

10. **Faça logout.**

- Se você definir "Permitir comunicação SSL/TLS" como [Somente texto cifrado], a comunicação não será possível caso seja selecionado um protocolo que não suporte um navegador da Web ou seja especificada apenas uma definição de grau de criptografia. Nesse caso, ative a comunicação definindo [Permitir comunicação SSL/TLS] como [Texto cifr/Texto n cript] utilizando o painel de controle do equipamento e, em seguida, especifique o protocolo e grau de criptografia corretos.
- É possível alterar as definições da versão SSL/TLS e do grau de criptografia, mesmo em [Segurança da rede].
- Dependendo dos estados que você especificar para "TLS1.2", "TLS1.1", "TLS1.0" e "SSL3.0", é possível que o equipamento não se conecte a um servidor LDAP externo.
- Os seguintes tipos de comunicação e dados são sempre criptografados por SSL3.0: comunicação via @Remote e os logs transferidos para o Remote Communication Gate S.

Definições de usuário para SSL/TLS

É recomendado que, após a instalação de um certificado autoassinado ou certificado de dispositivo de uma autoridade de certificação privada na unidade principal e após a ativação da função SSL/TLS (criptografia de comunicações), os usuários sejam instruídos a instalar o certificado em seus respectivos computadores. A instalação do certificado é especialmente necessária para usuários que queiram imprimir via IPP-SSL usando o Windows Vista/7/8/8.1, Windows Server 2008/2008 R2/2012/2012 R2. O administrador da rede deve instruir cada usuário para que instale o certificado.

Selecione [Trusted Root Certification Authorities] como o local de armazenamento de certificados quando acessar o equipamento usando IPP.

Nota

- Siga as etapas apropriadas ao receber uma dúvida de um usuário relacionada a problemas como certificado expirado.

- Se um certificado emitido por uma autoridade de certificado estiver instalado no equipamento, verifique o local de armazenamento do certificado com a autoridade de certificado.
- Para alterar o nome do host ou endereço IP em [Nome comum] do certificado de dispositivo ao utilizar a porta IPP padrão do sistema operacional no Windows Vista/7/8/8.1 ou Windows Server 2008/2008 R2/2012/2012 R2, exclua, primeiro, qualquer impressora anteriormente configurada no PC e reinstale-a depois de alterar o [Nome comum]. Além disso, para alterar as definições de autenticação do usuário (nome de usuário e senha de login), exclua, primeiro, qualquer impressora anteriormente configurada no PC e instale-a novamente depois de alterar as definições de autenticação do usuário.

Definir modo de criptografia SSL/TLS

Ao especificar o modo de comunicação criptografado SSL/TLS, é possível alterar os níveis de segurança.

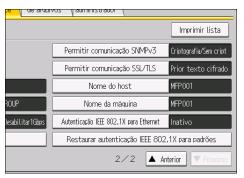
Modo de comunicação criptografada

Utilizando o modo de comunicação criptografada, é possível especificar comunicações criptografadas.

Modo de comunicação criptografada	Descrição
Somente texto cifrado	Permite apenas a comunicação criptografada. Se a criptografia não for possível, o equipamento não fará a comunicação.
Prioridade de texto cifrado	Executa a comunicação criptografada se a criptografia for possível. Se a criptografia não for possível, o equipamento faz a comunicação assim mesmo.
Texto cifr/Texto n cript	Faz a comunicação com ou sem criptografia, de acordo com as definições.

Depois de instalar um certificado de dispositivo, especifique o modo de comunicação criptografada SSL/TLS. Ao configurar esta definição, é possível alterar o nível de segurança.

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Definições de interface].**
4. **Pressione [▼Próximo].**

5. **Pressione [Permitir comunicação SSL/TLS].**

6. **Selecione o modo de comunicação criptografado desejado.**

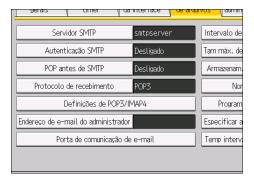
   Selecione [Somente texto cifrado], [Priorid de texto cifrado] ou [Texto cifr/Texto n cript] como o modo de comunicação criptografada.

7. **Pressione [OK].**
8. **Faça logout.**

- O modo de comunicação criptografada SSL/TLS também pode ser especificado utilizando o Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Ativar SSL para conexões SMTP

Utilize o procedimento seguinte para ativar a criptografia SSL para conexões SMTP.

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Transf de arquivos].**
4. **Pressione [Servidor SMTP].**

5. **Em "Usar conexão segura (SSL)", pressione [Ligado].**

   Se você não estiver usando SSL para conexões , pressione [Desligado].

   Quando a opção "Usar conexão segura (SSL)" é definida como [Ligado], o número da porta muda para 465.

6. **Pressione [OK].**
7. **Faça logout.**

Configurar S/MIME

Registrando um certificado de usuário no Catálogo de endereços, você pode enviar um e-mail criptografado com uma chave pública que evita que o conteúdo seja alterado durante a transmissão. Você também pode evitar a imitação de um remetente (spoofing) instalando um certificado de dispositivo no equipamento e anexando uma assinatura eletrônica criada com uma chave privada. Você pode aplicar estas funções separadamente ou, para maior segurança, em conjunto.

Para enviar e-mails criptografados, o remetente (este equipamento) e o destinatário devem suportar S/MIME.

- **Para utilizar S/MIME, é necessário especificar primeiro o [Endereço de e-mail do administrador] em [System Settings] (Definições do sistema).**

Aplicativos mensageiros compatíveis

A função S/MIME pode ser utilizada com os seguintes aplicativos:

- Microsoft Outlook 2003 e posterior
- Thunderbird 3.1.7 e posterior
- Windows Live Mail

- Se uma assinatura eletrônica for especificada para um e-mail, o endereço do administrador aparece no campo "De" e o endereço do usuário especificado como "remetente" aparece no campo "Responder a".
- Ao enviar e-mails para usuários cujos clientes de correio suportem S/MIME e usuários cujos clientes não suportem S/MIME, os e-mails para clientes S/MIME serão criptografados e os e-mails para clientes não-S/MIME serão enviados como texto simples.
- Ao utilizar S/MIME, o tamanho do e-mail é maior do que o normal.
- Para obter detalhes sobre a utilização de S/MIME com a função de scanner, consulte Digitalizar.

Criptografia de e-mail

Para enviar e-mail criptografados utilizando S/MIME, uma certificação de usuário deve primeiro ser preparada utilizando o Web Image Monitor e registrada no Catálogo de endereços pelo administrador de usuários. O registro do certificado no Catálogo de endereços especifica a chave pública de cada usuário. Depois de instalar o certificado, especifique o algoritmo de criptografia utilizando o Web Image Monitor. O administrador da rede pode especificar o algoritmo.

Criptografia de e-mail

1. Prepare um certificado de usuário.

2. Instale o certificado de usuário no Catálogo de endereços utilizando o Web Image Monitor. (A chave pública no certificado é especificada no Catálogo de endereços.)
3. Especifique o algoritmo de criptografia utilizando o Web Image Monitor.
4. Utilizando a chave compartilhada, criptografe a mensagem de e-mail.
5. A chave compartilhada é criptografada por meio da chave pública do usuário.
6. O e-mail criptografado é enviado.
7. O receptor descriptografa a chave compartilhada usando uma chave secreta que corresponde à chave pública.
8. O e-mail é descriptografado por meio da chave compartilhada.

- Existem 3 tipos de certificado de usuário que podem ser instalados neste equipamento: certificado "X.509 binário codificado por DER", "X.509 codificado em base 64", e "PKCS #7".
- Ao instalar um certificado de usuário no Catálogo de endereços utilizando o Web Image Monitor, talvez você veja uma mensagem de erro se o arquivo do certificado contiver mais de um certificado. Se este for o caso, instale os certificados um de cada vez.

Especificar o certificado de usuário

Prepare cada certificado de usuário antecipadamente.

1. **Faça login como administrador de usuários no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Catálogo de endereços].**
3. **Selecione o usuário para quem o certificado será instalado.**
4. **Clique em [Entrada detalhada] e em seguida clique em [Alterar].**

   A tela Alterar usuário é exibida.
5. **Insira o endereço do usuário no campo "Endereço de e-mail" em "E-mail".**
6. **Clique em [Alterar] em "Certificado de usuário".**
7. **Clique em [Procurar], selecione o arquivo do certificado de usuário e, em seguida, clique em [Abrir].**
8. **Clique em [OK].**

   O certificado de usuário é instalado.
9. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
10. **Faça logout.**

- Após o período válido do certificado de usuário selecionado, as mensagens criptografadas não poderão mais ser enviadas. Selecione um certificado que esteja dentro do período de validade.

Especificar o algoritmo de criptografia

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [S/MIME] em "Segurança".**
4. **Selecione o algoritmo de criptografia no menu suspenso ao lado de "Algoritmo de criptografia" em "Criptografia".**
5. **Clique em [OK].**

   O algoritmo para S/MIME é definido.

6. **Faça logout.**

- Configure as definições levando em consideração o algoritmo de criptografia e o algoritmo digest suportados pelo software de e-mail do usuário.

Anexar uma assinatura eletrônica

Para anexar uma assinatura eletrônica para enviar um e-mail, um certificado de dispositivo deve ser previamente instalado.

Como certificado de dispositivo, você pode usar um certificado autoassinado criado pela máquina ou um certificado emitido por uma autoridade de certificado. Para obter detalhes sobre como criar e instalar o certificado do dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo".

- Para instalar um certificado de dispositivo S/MIME, você deve primeiro registrar o "Endereço de e-mail do administrador" em [Definições do sistema] como o endereço de e-mail para o certificado de dispositivo. Observe que, mesmo que não utilize S/MIME, você deve especificar um endereço de e-mail para o certificado de dispositivo S/MIME.

Assinatura eletrônica

1. Instale um certificado de dispositivo no equipamento. A chave secreta do certificado é configurada no equipamento.
2. Anexe a assinatura eletrônica a um e-mail utilizando a chave secreta fornecida pelo certificado de dispositivo.

3. Envie o e-mail com a assinatura eletrônica anexada ao usuário.
4. O destinatário solicita a chave pública e o certificado de dispositivo da máquina.
5. Utilizando a chave pública, você pode determinar a autenticidade da assinatura eletrônica anexada para verificar se a mensagem foi alterada.

Fluxo da configuração (certificado autoassinado)

1. Crie e instale o certificado de dispositivo utilizando o Web Image Monitor.
2. Configures as definições do certificado a ser usado para S/MIME com o Web Image Monitor.
3. Configure as definições da assinatura eletrônica utilizando o Web Image Monitor.

Fluxo da configuração (certificado emitido por uma autoridade de certificação)

1. Crie o certificado de dispositivo utilizando o Web Image Monitor.

   O procedimento de solicitação para um certificado criado depende da autoridade de certificação. Siga o procedimento especificado pela autoridade de certificação.
2. Instale o certificado de dispositivo utilizando o Web Image Monitor.
3. Configures as definições do certificado a ser usado para S/MIME com o Web Image Monitor.
4. Configure as definições da assinatura eletrônica utilizando o Web Image Monitor.

Selecionar o certificado de dispositivo

Selecione o certificado de dispositivo a ser usado para S/MIME com o Web Image Monitor.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o certificado a ser utilizado para a assinatura eletrônica na caixa suspensa em "S/MIME" em "Certificação".**
5. **Clique em [OK].**

   O certificado a ser usado para a assinatura eletrônica S/MIME é definido.
6. **É apresentada a mensagem "Atualizando...". Aguarde de 1 a 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

- Se o certificado do dispositivo selecionado expirar, as assinaturas não poderão ser anexadas ao e-mail. Selecione um certificado que esteja dentro do período de validade.

Especificar a assinatura eletrônica

Depois de instalar um certificado de dispositivo no equipamento, configure as condições das assinaturas para S/MIME. O procedimento de configuração é o mesmo, independentemente do uso de um certificado autoassinado ou um certificado emitido por uma autoridade de certificação.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [S/MIME] em "Segurança".**
4. **Selecione o algoritmo digest a ser utilizado na assinatura eletrônica ao lado de "Algoritmo Digest" em "Assinatura".**
5. **Selecione o método para anexar a assinatura eletrônica ao enviar e-mail a partir do scanner ao lado de "Ao enviar e-mail pelo scanner" em "Assinatura".**
6. **Selecione o método para anexar a assinatura eletrônica ao encaminhar documentos armazenados ao lado de "Ao transferir arquivos armazenados no servidor de documentos (Utilitário)" em "Assinatura".**
7. **Clique em [OK].**

   As definições da assinatura eletrônica S/MIME são ativadas.
8. **Faça logout.**

- Configure as definições baseado no algoritmo de criptografia e no algoritmo digest suportados pelo software de e-mail do usuário.

Verificar o período de validade do certificado

O período de validade de um certificado usado com S/MIME é verificado quando o e-mail é enviado.

É possível alterar o momento de verificação do período de validade.

<table>
<tr><th>Modo de operação</th><th>Descrição</th></tr>
<tr><td>Prioridade de segurança</td><td>O período de validade é verificado nos seguintes momentos:
Certificado de usuário
(a) Quando o endereço é selecionado
(b) Quando a tecla [Iniciar] é pressionada
Certificado do dispositivo
(c) Quando o primeiro endereço é selecionado
(d) Quando a tecla [Iniciar] é pressionada</td></tr>
<tr><td>Prioridade de desempenho</td><td>As ações (b) e (c) são omitidas.
A verificação do período de validade poderá demorar mais se o endereço estiver selecionado ou a tecla [Iniciar] for pressionada. Para reduzir o tempo, selecione "Prioridade de desempenho".</td></tr>
</table>

5

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [S/MIME] em "Segurança".**
4. **Em "Modo de operação", selecione [Prioridade de Segurança] ou [Prioridade de desempenho].**
5. **Clique em [OK].**
6. **Faça logout.**

- Se um certificado era válido quando foi transmitido, mas expirou antes de recuperar o e-mail do servidor de e-mails para o computador cliente, o e-mail não poderá ser recuperado.
- Caso ocorra um erro fora do período de validade quando um e-mail S/MIME for enviado automaticamente utilizando a transmissão de memória ou em um determinado momento, o erro é reportado com um e-mail em texto simples para o endereço de e-mail do remetente ou administrador. Os detalhes do erro podem ser visualizados no registro de trabalhos. Ao usar S/MIME, certifique-se de ativar a função de coleta de registro de trabalhos. Para obter detalhes sobre a exibição de logs, consulte Pág. 193 "Gerenciar arquivos de log".

Configuração de PDFs com assinaturas eletrônicas

Este equipamento pode criar PDFs com assinaturas eletrônicas. PDFs com assinaturas eletrônicas certificam o criador do documento PDF e a data e hora da criação. Também é possível evitar a violação com a detecção dos documentos violados.

Para criar PDFs com assinaturas eletrônicas, selecione primeiro o certificado a ser usado para a assinatura entre os certificados de dispositivo criados e instalados.

Como certificado de dispositivo, você pode usar um certificado autoassinado criado pela máquina ou um certificado emitido por uma autoridade de certificado. Para obter mais informações sobre como criar e instalar um certificado de dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo".

- Para criar PDFs assinados digitalmente, você deve primeiro especificar o [Endereço de e-mail do administrador] em [Transf de arquivos] em [Definições do sistema].
- Para usar o certificado do dispositivo para PDFs assinados digitalmente, você deve primeiro especificar o endereço de e-mail do administrador igual àquele registrado em "Endereço de e-mail do administrador" nas [Definições do sistema].

Selecione o certificado a ser utilizado para as assinaturas.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o certificado a ser utilizado para a assinatura eletrônica na caixa suspensa em "Assinatura digital de PDF" ou "Assinatura digital de PDF/A" em "Certificação".**

   Assinatura digital de PDF: Podem ser anexadas aos PDFs em outros formatos além do PDF/A.

   Assinatura digital de PDF/A: Podem ser anexadas aos PDFs no formato PDF/A.
5. **Clique em [OK].**
6. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

- Se o certificado de dispositivo selecionado expirar, as assinaturas não poderão ser anexadas a PDFs. Selecione um certificado que esteja dentro do período de validade.

- O algoritmo de assinatura para a assinatura digital do certificado de dispositivo que pode ser anexado aos arquivos PDF/A é "sha1WithRSA-1024".

Configurar definições IPsec

Para a segurança das comunicações, este equipamento suporta IPsec. O IPsec transmite pacotes de dados seguros ao nível de protocolo IP utilizando o método de chave de criptografia compartilhada, no qual o remetente e o destinatário possuem a mesma chave. Este equipamento utiliza a troca automática de chaves para configurar chaves pré-compartilhadas por ambas as partes.
Utilizando a definição de troca automática, você pode renovar as definições de troca de chave compartilhada dentro de um período de tempo específico, garantindo, assim, maior segurança na transmissão.

- Quando for especificado "Inativo" para "Excluir comunicação HTTPS ", o acesso ao Web Image Monitor pode ser perdido se as definições de chave estiverem configuradas de forma incorreta. Para evitar que isso, você pode especificar o IPsec para excluir a transmissão HTTPS selecionando "Ativo". Se desejar incluir a transmissão HTTPS, recomendamos que selecione "Inativo" para "Excluir a comunicação HTTPS" após verificar se o IPsec está devidamente configurado. Quando "Ativo" estiver selecionado para "Excluir comunicação HTTPS", apesar de a transmissão HTTPS não ser abrangida pelo IPsec, o Web Image Monitor poderá ficar inacessível quando o TCP for abrangido pelo IPsec no computador.
- Se você não conseguir acessar o Web Image Monitor devido a problemas de configuração do IPsec, desative o IPsec nas Definições do sistema no painel de controle e, em seguida, acesse o Web Image Monitor.
- Para mais informações sobre ativação e desativação do IPsec utilizando o painel de controle, consulte Connecting the Machine/ System Settings.
- O IPsec não é aplicado a dados obtidos através de DHCP, DNS ou WINS.

Sistemas operacionais suportados

Sistema operacional	Nota
• Windows Server 2003/2003 R2	IPsec sobre IPv4 pode ser usado.
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 ou posterior • Red Hat Enterprise Linux WS 4.0 • Solaris 10	IPsec sobre IPv4 e IPv6 pode ser usado.

Dependendo do sistema operacional, alguns itens de definição não são suportados. Certifique-se de que as definições IPsec que você especificar sejam consistentes com as definições IPsec do sistema operacional.

Criptografia e autenticação por IPsec

O IPsec consiste em 2 funções principais: a função de criptografia, que assegura a confidencialidade dos dados, e a função de autenticação, que verifica o remetente e a integridade dos dados. A função IPsec deste equipamento suporta 2 protocolos de segurança: o protocolo ESP, que ativa as duas funções do IPsec ao mesmo tempo, e o protocolo AH, que ativa apenas a função de autenticação.

Protocolo ESP

O protocolo ESP oferece uma transmissão segura através de autenticação e criptografia. Este protocolo não fornece autenticação do cabeçalho.

- Para uma criptografia bem-sucedida, o remetente e o destinatário devem especificar o mesmo algoritmo de criptografia e chave de criptografia. Se você utilizar o método de troca automática de chave de criptografia, o algoritmo de criptografia e a chave de criptografia são especificados automaticamente.
- Para uma autenticação bem-sucedida, o remetente e o destinatário devem especificar o mesmo algoritmo de autenticação e chave de autenticação. Se você utilizar o método de troca automática de chave de criptografia, o algoritmo de autenticação e a chave autenticação são especificados automaticamente.

Protocolo AH

O protocolo AH oferece uma transmissão segura através da autenticação exclusiva de pacotes, incluindo cabeçalhos.

- Para uma autenticação bem-sucedida, o remetente e o destinatário devem especificar o mesmo algoritmo de autenticação e chave de autenticação. Se você utilizar o método de troca automática de chave de criptografia, o algoritmo de autenticação e a chave autenticação são especificados automaticamente.

Protocolo AH + protocolo ESP

Quando combinados, os protocolos ESP e AH oferecem uma transmissão segura através de criptografia e autenticação. Estes protocolos oferecem autenticação de cabeçalho.

- Para uma criptografia bem-sucedida, o remetente e o destinatário devem especificar o mesmo algoritmo de criptografia e chave de criptografia. Se você utilizar o método de troca automática de chave de criptografia, o algoritmo de criptografia e a chave de criptografia são especificados automaticamente.
- Para uma autenticação bem-sucedida, o remetente e o destinatário devem especificar o mesmo algoritmo de autenticação e chave de autenticação. Se você utilizar o método de troca automática de chave de criptografia, o algoritmo de autenticação e a chave autenticação são especificados automaticamente.

- Alguns sistemas operacionais utilizam o termo "Conformidade" em vez de "Autenticação".

Definições de troca automática de chave de criptografia

Para configuração da chave, este equipamento suporta a troca automática de chave para especificar combinações, como chave e algoritmo IPsec para o remetente e o destinatário.

Combinações como essas formam o que se chama de SA (Security Association). A comunicação IPsec só é possível se as definições SA do destinatário e do remetente forem idênticas.

Se você utilizar o método de troca automática para especificar a chave de criptografia, as definições SA são configuradas automaticamente nos equipamentos de ambas as partes. No entanto, antes de definir o SA do IPsec, as definições SA ISAKMP (Fase 1) são feitas automaticamente. Depois disto, as definições SA do IPsec (Fase 2), que permitem a transmissão IPsec, são feitas automaticamente.

Além disso, para maior segurança, o SA pode ser atualizado de forma automática periodicamente aplicando um período de validade (limite de tempo) para as suas definições. Este equipamento suporta apenas IKEv1 para a troca automática de chave de criptografia.

É possível configurar múltiplos SAs.

Definições 1 a 4 e definição padrão

Utilizando o método de troca automática, é possível configurar quatro conjuntos distintos de detalhes SA (como chaves compartilhadas e algoritmos IPsec diferentes). Nas definições padrão desses conjuntos, você pode incluir definições não abrangidas pelos campos dos conjuntos 1 a 4.

Quando IPsec estiver ativado, o conjunto 1 tem maior prioridade, e o conjunto 4, menor prioridade. Você pode utilizar esse sistema de prioridades para acessar endereços IP de forma mais segura. Por exemplo, defina o maior intervalo IP para a prioridade mais baixa (4) e depois defina endereços IP específicos para um nível de prioridade mais elevado (3 e superior). Desse modo, quando a transmissão IPsec for ativada para um endereço IP específico, serão aplicadas as definições de nível mais elevado.

Definições de IPsec

As definições IPsec para este equipamento podem ser efetuadas no Web Image Monitor. A tabela a seguir explica os itens individuais de definição.

Itens das definições de IPsec

Definição	Descrição	Valor da definição
IPsec	Especifique se deseja ou não ativar o IPsec.	• Ativo • Inativo

Definição	Descrição	Valor da definição
Excluir comunicação HTTPS	Especifique se deseja ativar o IPsec para a transmissão HTTPS.	• Ativo • Inativo Especifique "Ativo" se não quiser utilizar IPsec para transmissão HTTPS.

A definição IPsec pode também ser configurada a partir do painel de controle.

Nível de segurança de troca automática de chave de criptografia

Quando você seleciona o nível de segurança, algumas definições de segurança são configuradas automaticamente. A tabela seguinte explica as funções dos níveis de segurança.

Nível de segurança	Características do nível de segurança
Somente autenticação	Selecione esse nível se quiser autenticar o interlocutor da transmissão e evitar a alteração não autorizada dos dados, mas sem executar a criptografia do pacote de dados. Como os dados são enviados em texto não criptografado, os pacotes de dados são vulneráveis a ataques de escuta. Não selecione essa opção se estiver trocando informações confidenciais.
Autenticação e criptografia de baixo nível	Selecione esse nível se quiser criptografar os pacotes de dados e autenticar o interlocutor da transmissão e evitar a alteração não autorizada do pacote. A criptografia de pacotes ajuda a evitar os ataques de escuta. Esse nível oferece menos segurança que "Autenticação e criptografia de alto nível".
Definição concluída	Selecione esse nível se quiser criptografar os pacotes de dados e autenticar o interlocutor da transmissão e evitar a alteração não autorizada do pacote. A criptografia de pacotes ajuda a evitar os ataques de escuta. Esse nível oferece maior segurança que "Autenticação e criptografia de baixo nível".

A tabela seguinte lista as definições que são configuradas automaticamente de acordo com o nível de segurança.

Definição	Somente autenticação	Autenticação e criptografia de baixo nível	Definição concluída
Política de segurança	Aplicar	Aplicar	Aplicar
Modo de encapsulamento	Transportar	Transportar	Transportar
Nível de requisito IPsec	Usar quando possível	Usar quando possível	Sempre requerer
Método de autenticação	PSK	PSK	PSK
Fase 1 Algoritmo Hash	MD5	SHA1	SHA256
Fase 1 Algoritmo de encriptação	DES	3DES	AES-128-CBC
Fase 1 Grupo Diffie-Hellman	2	2	2
Fase 2 Protocolo de segurança	AH	ESP	ESP
Fase 2 Algoritmo de autenticação	HMAC-SHA1-96/ HMAC- -SHA256-128/ HMAC- -SHA384-192/ HMAC- -SHA512-256	HMAC-SHA1-96/ HMAC- -SHA256-128/ HMAC- -SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
Fase 2 Permissões de algoritmo de criptografia	Texto claro (Encriptação NULL)	3DES/AES-128/ AES-192/AES-256	AES-128/AES-192/ AES-256
Fase 2 PFS	Inativo	Inativo	2

Itens de definições de troca automática de chave de criptografia

Quando especifica um nível de segurança, as definições de segurança correspondentes são configuradas automaticamente, mas outras definições, tal como o tipo de endereço, endereço local e endereço remoto, continuam a ter de ser definidas manualmente.

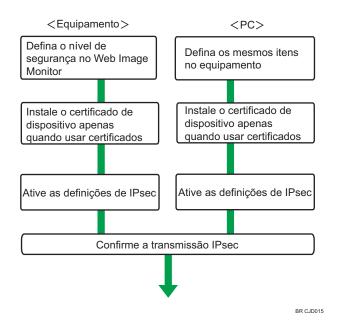
Depois de especificar um nível de segurança, você ainda pode fazer alterações nas definições configuradas automaticamente. Quando você altera uma definição configurada automaticamente, o nível de segurança muda automaticamente para "Definição de usuário".

Definição	Descrição	Valor da definição
Tipo de endereço	Especifique o tipo de endereço para o qual é utilizada a transmissão IPsec.	• Inativo • IPv4 • IPv6 • IPv4/IPv6 (apenas Definições padrão)
Endereço local	Especifique o endereço do equipamento. Se estiver a utilizar vários endereços IPv6, pode também especificar um intervalo de endereços.	O endereço IPv4 ou IPv6 do equipamento. Se você não definir um intervalo de endereços, insira 32 depois de um endereço IPv4 ou 128 depois de um endereço IPv6.
Endereço remoto	Especifique o endereço do interlocutor da transmissão IPsec. Você também pode especificar um intervalo de endereços.	O endereço IPv4 ou IPv6 do interlocutor da transmissão IPsec. Se você não definir um intervalo de endereços, insira 32 depois de um endereço IPv4 ou 128 depois de um endereço IPv6.
Política de segurança	Especifique como o IPsec é tratado.	• Aplicar • Ignorar • Descartar

Definição	Descrição	Valor da definição
Modo de encapsulamento	Especifique o modo de encapsulamento. (definição automática)	• Transportar • Túnel Se você especificar "Túnel", deverá, em seguida, especificar "Terminal de túnel", que consiste em endereços IP de início e fim. Para o ponto de início, defina o endereço definido em "Endereço local".
Nível de requisito IPsec	Especifique se deseja transmitir apenas através de IPsec ou permitir a transmissão de texto não criptografado quando não for possível estabelecer o IPsec. (definição automática)	• Usar quando possível • Sempre requerer
Método de autenticação	Especifique o método de autenticação para os interlocutores da transmissão. (definição automática)	• PSK • Certificate Se você especificar "PSK", deverá, em seguida, definir o texto PSK (utilizando caracteres ASCII). Se estiver usando "PSK", especifique uma senha PSK utilizando até 32 caracteres ASCII. Se você especificar "Certificate", a certificação para IPsec deverá de ser instalada e especificada para que possa ser usada.
Texto PSK	Especificar a chave pré--compartilhada para autenticação PSK.	Insira a chave pré--compartilhada necessária para a autenticação PSK.

Definição	Descrição	Valor da definição
Fase 1 Algoritmo hash	Especifique o algoritmo hash a ser utilizado na fase 1. (definição automática)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
Fase 1 Algoritmo de criptografia	Especifique o algoritmo de encriptação a ser utilizado na fase 1. (definição automática)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
Fase 1 Grupo Diffie-Hellman	Selecione o número do grupo Diffie-Hellman utilizado para geração de chave de criptografia IKE. (definição automática)	• 1 • 2 • 14
Fase 1 Período de validade	Especifique o período de tempo pelo qual as definições SA na fase 1 serão válidas.	Defina, em segundos, de 300 seg. (5 min.) a 172800 seg. (48 horas).
Fase 2 Protocolo de segurança	Especifique o protocolo de segurança a ser utilizado na fase 2. Para aplicar a encriptação e a autenticação a dados enviados, especifique o "ESP" ou o "ESP+AH". Para aplicar apenas dados de autenticação, especifique o "AH". (definição automática)	• ESP • AH • ESP+AH

Definição	Descrição	Valor da definição
Fase 2 Algoritmo autenticador	Especifique o algoritmo de autenticação a ser utilizado na fase 2. (definição automática)	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Fase 2 Permissões de algoritmo de criptografia	Especifique o algoritmo de encriptação a ser utilizado na fase 2. (definição automática)	• Texto claro (Encriptação NULL) • DES • 3DES • AES-128 • AES-192 • AES-256
Fase 2 PFS	Especifique se deseja ativar PFS. De seguida, se PFS estiver ativado, selecione o grupo Diffie-Hellman. (definição automática)	• Inativo • 1 • 2 • 14
Fase 2 Período de validade	Especifique o período de tempo pelo qual as definições SA na fase 2 serão válidas.	Especifique um período (em segundos) de 300 (5 min.) a 172800 (48 h).

Definições de troca automática de chave de criptografia Fluxo de configuração

- Para utilizar um certificado para autenticar o interlocutor da transmissão nas definições de chave de encriptação negociada automaticamente, é necessário encontrar-se instalado um certificado do dispositivo.
- Depois de configurar o IPsec, você poderá utilizar o comando "Ping" para verificar se a conexão foi devidamente estabelecida. No entanto, não pode utilizar o comando "Ping" quando ICMP é excluído da transmissão IPsec por parte do computador. Além disso, uma vez que a resposta é lenta durante a negociação inicial da chave, poderá demorar algum tempo a confirmar que a transmissão foi estabelecida.

Especificar Definições do código de encriptação negociado automaticamente

Para alterar o método de autenticação do interlocutor da transmissão para as definições de código de encriptação negociado automaticamente para "Certificação", primeiro deve instalar e atribuir uma certificação. Para obter mais informações sobre como criar e instalar um certificado de dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo". Para o método de atribuição de certificados instalados no IPsec, consulte Pág. 148 "Selecionar o certificado para IPsec".

1. Faça login como administrador da rede no Web Image Monitor.

2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique na opção [IPsec] em "Segurança".**
4. **Clique na opção [Editar] em "Definições de troca automática de chave de criptografia".**
5. **Faça as definições de troca automática de chave de criptografia em [Definições 1].**

   Se quiser fazer várias definições, selecione o número de definições e adicione as definições.
6. **Clique em [OK].**
7. **Selecione [Ativo] para " IPsec" em "IPsec".**
8. **Defina "Excluir comunicação HTTPS" como [Ativo] se não quiser utilizar o IPsec para transmissão HTTPS.**
9. **Clique em [OK].**
10. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

    Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
11. **Faça logout.**

Selecionar o certificado para IPsec

Utilizando o Web Image Monitor, selecione o certificado a ser utilizado para IPsec. É necessário instalar o certificado antes de poder ser utilizado. Para obter mais informações sobre como criar e instalar um certificado de dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo".

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o certificado a ser utilizado para o IPsec na caixa suspensa em "IPsec" em "Certificação".**
5. **Clique em [OK].**

   O certificado para IPsec é especificado.
6. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

Especificar as definições de IPsec do computador

Configure as definições de SA de IPsec do computador de modo que coincidam exatamente com o nível de segurança da equipamento no equipamento. Os métodos de definição diferem de acordo com o sistema operativo do computador. O procedimento de exemplo apresentado aqui utiliza o Windows 7 quando o nível de segurança "Autenticação e criptografia de nível baixo" se encontra selecionado.

1. **No menu [Iniciar], clique em [Painel de controle], clique em [Sistema e segurança] e, em seguida, clique em [Ferramentas administrativas].**

   No Windows 8, coloque o cursor do mouse sobre o canto superior ou inferior direito da tela e clique em [Definições], [Painel de Controle], [Sistema e Segurança] e em [Ferramentas Administrativas].

2. **Clique duas vezes em [Política de segurança local].**

   Se aparecer a caixa de diálogo "Controle da conta do usuário", clique em [Sim].

3. **Clique em [Políticas de Segurança IP no Computador Local].**
4. **No menu "Ação", clique em [Criar Política de Segurança IP].**

   Aparece o Assistente da Política de Segurança IP.

5. **Clique em [Próximo].**
6. **Introduza um nome para a política de segurança em "Nome" e clique em [Seguinte].**
7. **Desmarque a caixa de seleção "Ativar a regra de resposta padrão" e clique em [Próximo].**
8. **Selecione "Editar propriedades" e clique em [Concluir].**
9. **Na guia "Geral", clique em [Definições].**
10. **Em "Autenticar e criar um novo código a cada", introduza o mesmo período de validade (em minutos) que é especificado no equipamento em "Definições de troca automática de chave de criptografia Fase 1", e, em seguida, clique em [Métodos].**
11. **Certifique-se que as definições do algoritmo hash ("Integridade"), algoritmo de criptografia ("Criptografia") e "Grupo Diffie-Helman" em "Ordem de preferência dos métodos de segurança" correspondam às definições especificadas no equipamento em "Definições de troca automática de chave de criptografia Fase 1".**

    Se as definições não forem apresentadas, clique em [Adicionar].

12. **Clique duas vezes em [OK].**
13. **Clique em [Adicionar] no separador "Regras".**

    Aparece o Assistente de Regras de Segurança.

14. **Clique em [Próximo].**
15. **Selecione "Esta regra não especifica um encapsulamento" e clique em [Próximo].**
16. **Selecione o tipo de rede para IPsec e clique em [Próximo].**

17. **Clique em [Adicionar] na Lista de Filtros IP.**
18. **Em [Nome], introduza um nome de Filtro IP e clique em [Adicionar].**

    Aparece o Assistente de Filtro IP.
19. **Clique em [Próximo].**
20. **Se necessário, insira uma descrição do filtro IP, e, em seguida, clique em [Próximo].**
21. **Selecione "Meu endereço IP" em "Endereço de origem" e, em seguida, clique em [Próximo].**
22. **Selecione "Um endereço IP ou sub-rede específica" em "Endereço de destino", introduza o endereço IP do equipamento e então clique em [Próximo].**
23. **Selecione o tipo de protocolo para IPsec e depois clique em [Próximo].**

    Se estiver utilizando IPsec com IPv6, selecione "58" como número de protocolo para o tipo de protocolo-alvo "Outro".

24. **Clique em [Concluir].**
25. **Clique em [OK].**
26. **Selecione o filtro IP que você acabou de criar e, em seguida, clique em [Próximo].**
27. **Clique em [Add] (Adicionar).**

    Aparece o assistente de ação de filtro.
28. **Clique em [Próximo].**
29. **Em [Nome], insira um nome de ação de Filtro IP e clique em [Próximo].**
30. **Selecione "Negociar segurança" e clique em [Próximo].**
31. **Selecione "Permitir comunicação não segura se não for possível uma conexão segura.", e, em seguida, clique em [Próximo].**
32. **Selecione "Personalizado" e clique em [Configurações].**
33. **Em "Algoritmo de integridade", selecione o algoritmo de autenticação que foi especificado no equipamento em Definições de troca automática de chave de criptografia Fase 2".**
34. **Em "Algoritmo de criptografia", selecione o algoritmo de criptografia que está especificado no equipamento em "Definições de troca automática de chave de criptografia Fase 2".**
35. **Em "Configurações de chave de sessão:", selecione "GerGerar nova chave a cada" e insira o período de validade (em segundos) que foi especificado no equipamento nas "Definições de troca automática de chave de criptografia em Fase 2".**
36. **Clique em [OK].**
37. **Clique em [Próximo].**
38. **Clique em [Concluir].**

39. **Selecione a ação do filtro recém-criado e, em seguida, clique em [Próximo].**

    Se você definir "Definições de troca automática de chave de criptografia" como "Autenticação e criptografia de alto nível", selecione a ação de filtro IP que acaba de ser criada, clique em [Editar] e, em seguida, marque "Usar sigilo total na transferência de chave de sessão (PFS)" na caixa de diálogo de propriedades de ação do filtro.

    Se você utilizar o PFS no Windows, o número de grupo PFS utilizado na fase 2 é negociado automaticamente na fase 1 a partir do número de grupo Diffie-Hellman (definido na etapa 11). Consequentemente, se alterar as definições automáticas especificadas do nível de segurança no equipamento e aparecer "Definição do utilizador", deve definir o mesmo número de grupo para a "Fase 1 do Grupo Diffie-Hellman" e "Fase 2 PFS" no equipamento para estabelecer a transmissão IPsec.

40. **Selecione o método de autenticação e, em seguida, clique em [Próximo].**

    Se selecionar "Certificação" como o método de autenticação em "Definições de troca automática de chave de criptografia" no equipamento, especifique o certificado do dispositivo. Se você selecionar "PSK", insira o mesmo texto PSK especificado no equipamento com a chave pré--compartilhada.

41. **Clique em [Concluir].**
42. **Clique em [OK].**

    A nova política de segurança IP (definições IPsec) está especificada.

43. **Selecione a política de segurança que você acabou de criar, clique com o botão direito do mouse e clique em [Atribuir].**

    As definições de IPsec do computador estão habilitadas.

- Para desabilitar as definições IPsec do computador, selecione a política de segurança, clique com o botão direito do mouse e, em seguida, clique em [Cancelar atribuição].

Comandos de definição telnet

É possível utilizar telnet para confirmar as definições IPsec e alterar as definições. Esta seção explica os comandos telnet para IPsec. Para obter informações sobre o nome de usuário e a senha de login no telnet, consulte o administrador. Para obter informações sobre login no telnet e operações telnet, consulte Connecting the Machine/ System Settings.

- **Se utilizar um certificado como método de autenticação nas definições de chave de encriptação negociada automaticamente (IKE), instale o certificado utilizando o Web Image Monitor. Não é possível instalar um certificado utilizando telnet.**

ipsec

Para visualizar informações de definições relacionadas com IPsec, utilize o comando "ipsec".

Exibir as definições atuais

```
msh> ipsec
```

Apresenta as seguintes informações sobre definições IPsec:

- Valores das definições IPsec
- Definições manuais da chave de encriptação, valores de definição IKE 1-4
- Definições manuais da chave de encriptação, valores predefinidos IKE

Exibir as partes das definições atuais

```
msh> ipsec -p
```

- Apresenta as informações sobre definições IPsec em partes.

ipsec exclude

Para visualizar ou especificar os protocolos excluídos por IPsec, utilize o comando "ipsec exclude".

Exibir as definições atuais

```
msh> ipsec exclude
```

- Exibe os protocolos atualmente excluídos da transmissão IPsec.

Especificar os protocolos a excluir

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Especifique o protocolo e insira [on] para excluí-lo ou [off] para incluí-lo na transmissão IPsec. Se você inserir [all], todos os protocolos serão especificados em conjunto.

ipsec ike

Para visualizar ou especificar as definições de código de encriptação negociado automaticamente, utilize o comando "ipsec ike".

Exibir as definições atuais

```
msh> ipsec ike {1|2|3|4|default}
```

- Para visualizar as definições 1-4, especifique o número [1-4].
- Para visualizar a predefinição, especifique [default].
- Não especificar nenhum valor apresenta todas as definições.

Desactivar definições

```
msh> ipsec ike {1|2|3|4|default} disable
```

- Para desactivar as definições 1-4, especifique o número [1-4].

- Para desactivar as predefinições, especifique [default].

Especifique o endereço local/endereço remoto específico do usuário.

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Introduza o número da definição individual [1-4] e o tipo de endereço para especificar o endereço local e remoto.
- Para definir os valores de endereço local ou remoto, especifique masklen introduzindo [/] e um número inteiro de 0 a 32 aquando da definição de um endereço IPv4. Na definição de um endereço IPv6, especifique masklen introduzindo [/] e um número inteiro de 0 a 128.
- Se nenhum valor de endereço for especificado, a definição atual será exibida.

Especificar o tipo de endereço na predefinição

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Especifique o tipo de endereço para a predefinição.
- Para especificar IPv4 e IPv6, introduza [any].

Definição da política de segurança

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Insira o número da definição individual [1-4] ou [default] e especifique a política de segurança para o endereço especificado na definição selecionada.
- Para aplicar IPsec aos pacotes relevantes, especifique [apply]. Para não aplicar IPsec, especifique [bypass].
- Se especificar [discard], são descartados todos os pacotes aos quais seja possível aplicar o IPsec.
- Se nenhuma política de segurança for especificada, a definição atual será exibida.

Definição do protocolo de segurança

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o protocolo de segurança.
- Para especificar AH, introduza [ah]. Para especificar ESP, introduza [esp]. Para especificar AH e ESP, introduza [dual].
- Se nenhum protocolo for especificado, a definição atual será exibida.

Definição do nível de requisito IPsec

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o nível de requisito IPsec.
- Se especificar [require], os dados não serão transmitidos se não for possível utilizar o IPsec. Se especificar [use], os dados serão enviados normalmente se não for possível utilizar o IPsec. Quando for possível utilizar IPsec, é executada a transmissão IPsec.

- Se nenhum nível de requisito for especificado, a definição atual será exibida.

Definição do modo de encapsulamento

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o modo de encapsulamento.
- Para especificar o modo de transporte, introduza [transport]. Para especificar o modo de túnel, introduza [tunnel].
- Se tiver definido o tipo de endereço na predefinição para [any], não é possível utilizar [tunnel] no modo de encapsulamento.
- Se nenhum modo de encapsulamento for especificado, a definição atual será exibida.

Definição de ponto de término de encapsulamento

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP address"
```


- Introduza o número da definição individual [1-4] ou [default] e especifique o endereço IP de início e de fim do ponto de fim de túnel.
- Se o endereço de início ou fim não for especificado, a definição atual será exibida.

Definição do método de autenticação do interlocutor IKE

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o método de autenticação.
- Especifique [psk] para utilizar uma chave partilhada como método de autenticação. Especifique [rsasig] para utilizar um certificado como método de autenticação.
- Se você selecionar [psk], deverá especificar a cadeia de caracteres PSK.
- Note que se você selecionar "Certificado", é necessário instalar e especificar o certificado para IPsec antes de poder utilizá-lo. Para instalar e especificar o certificado utilize o Web Image Monitor.

Definição da cadeia de caracteres PSK

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- Se você selecionar PSK como método de autenticação, insira o número da definição individual [1-4] ou [default] e especifique a cadeia de caracteres PSK.
- Especifique a cadeia de caracteres ASCII. Não são permitidas abreviaturas.

Definição do algoritmo hash de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo hash de SA ISAKMP (fase 1).
- Se nenhum algoritmo hash for especificado, a definição atual será exibida.

Definição do algoritmo de encriptação de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de encriptação de SA ISAKMP (fase 1).
- Se nenhum algoritmo de criptografia for especificado, a definição atual será exibida.

Definição do grupo Diffie-Hellman de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o número do grupo Diffie-Hellman de SA ISAKMP (fase 1).
- Especifique o número de grupo a ser utilizado.
- Se nenhum número de grupo for especificado, a definição atual será exibida.

Definição do período de validade de SA ISAKMP (fase 1)

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o período de validade de SA ISAKMP (fase 1).
- Introduza o período de validade (em segundos) de 300 a 172800.
- Não especificar um período de validade apresenta a definição actual.

Definição do algoritmo de autenticação de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-
-sha384|hmac-sha512}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de autenticação de SA IPsec (fase 2).
- Separe as entradas de vários algoritmos de encriptação com uma vírgula (,). Os valores de definição atuais são apresentados pela ordem de maior prioridade.
- Se nenhum algoritmo de autenticação for especificado, a definição atual será exibida.

Definição do algoritmo de encriptação de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|
aes256}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o algoritmo de encriptação de SA IPsec (fase 2).
- Separe as entradas de vários algoritmos de encriptação com uma vírgula (,). Os valores de definição atuais são apresentados pela ordem de maior prioridade.
- Se nenhum algoritmo de criptografia for especificado, a definição atual será exibida.

Definição PFS de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o número do grupo Diffie-Hellman de SA IPsec (fase 2).
- Especifique o número de grupo a ser utilizado.
- Se nenhum número de grupo for especificado, a definição atual será exibida.

Definição do período de validade de SA IPsec (fase 2)

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- Introduza o número da definição individual [1-4] ou [default] e especifique o período de validade de SA IPsec (fase 2).
- Introduza o período de validade (em segundos) de 300 a 172800.
- Não especificar um período de validade apresenta a definição actual.

Repor os valores de definição

```
msh> ipsec ike {1|2|3|4|default|all} clear
```


- Insira o número da definição individual [1-4] ou [default] e redefina a definição especificada. A especificação de [all] redefine todas as definições, incluindo as predefinições.

Configurar a autenticação IEEE 802.1X

IEEE 802.1X é um padrão de autenticação e utiliza o servidor de autenticação (servidor RADIUS).

É possível selecionar 4 tipos de método de autenticação EAP: EAP-TLS, LEAP, EAP-TTLS e PEAP. Observe que cada método de autenticação EAP tem diferentes definições e procedimentos de autenticação.

Os tipos e os requisitos relativos aos certificados são os seguintes:

Tipo de EAP	Certificados necessários
EAP-TLS	Certificado do site, certificado do dispositivo (certificado do cliente IEEE 802.1X)
LEAP	-
EAP-TTLS	Certificado do site
PEAP	Certificado do site
PEAP (a Fase 2 destina-se apenas a TLS)	Certificado do site, certificado do dispositivo (certificado do cliente IEEE 802.1X)

Instalar um certificado de site

Instale um certificado de site (certificado de raiz CA) para verificação da confiabilidade do servidor de autenticação. É necessário ter pelo menos um certificado emitido pela autoridade de certificado que assinou o certificado de servidor ou um certificado de uma autoridade de certificação mais alta.

Apenas certificados de site PEM (X.509 codificado para Base64) podem ser importados.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado do site] em "Segurança".**
4. **Clique em [Procurar] para "Certificado do site a ser importado" e, em seguida, selecione o certificado de CA obtido.**
5. **Clique em [Abrir].**
6. **Clique em [Importar].**
7. **Verifique se o [Status] do certificado importado indica "Confiável".**

   Se a [Verificação do Certificado do site] estiver no modo [Ativo] e o [Status] do certificado for [Não confiável], a comunicação talvez não seja possível.
8. **Clique em [OK].**

9. **Faça logout.**

Selecionar o Certificado de dispositivo

Selecione o certificado desejado em IEEE 802.1X entre os certificados de dispositivo criados e instalados previamente no equipamento. Para obter mais informações sobre como criar e instalar um certificado de dispositivo, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo".

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Certificado de dispositivo] no menu "Segurança".**
4. **Selecione o certificado a ser utilizado para IEEE 802.1X na caixa suspensa em "IEEE 802.1X" em "Certificação".**
5. **Clique em [OK].**
6. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
7. **Faça logout.**

Definir itens de IEEE 802.1X para Ethernet

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique na opção [IEEE 802.1X] em "Segurança".**
4. **Em "Nome de usuário", insira o nome de usuário definido no servidor RADIUS.**
5. **Insira o nome de domínio em "Nome de domínio".**
6. **Selecione "Tipo de EAP". As configurações variam de acordo com o Tipo de EAP.**

   EAP-TLS

   - Execute as seguintes definições de acordo com o sistema operacional a ser utilizado:
     - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
     - Selecione [Ligado] ou [Desligado] em "Confiar na autoridade de certificação intermediária".
     - Insira o nome de host do servidor RADIUS em "ID do servidor".
     - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

LEAP

- Clique em [Alterar] em "Senha" e, em seguida, insira a senha definida no servidor RADIUS.

EAP-TTLS

- Clique em [Alterar] em "Senha" e, em seguida, insira a senha definida no servidor RADIUS.
- Clique em [Alterar] em "Nome de usuário da fase 2" e, em seguida, insira o nome de usuário definido no servidor RADIUS.
- Selecione [CHAP], [MSCHAP], [MSCHAPv2], [PAP] ou [MD5] em "Método da fase 2".

  Alguns métodos podem não estar disponíveis, dependendo do servidor RADIUS que deseja usar.
- Execute as seguintes definições de acordo com o sistema operacional a ser utilizado:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Confiar na autoridade de certificação intermediária".
  - Insira o nome de host do servidor RADIUS em "ID do servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

PEAP

- Clique em [Alterar] em "Senha" e, em seguida, insira a senha definida no servidor RADIUS.

  Se [TLS] estiver selecionado para "Método da fase 2", você não precisa especificar uma senha.
- Clique em [Alterar] em "Nome de usuário da fase 2" e, em seguida, insira o nome de usuário definido no servidor RADIUS.
- Selecione [MSCHAPv2] ou [TLS] em "Método da fase 2".

  Quando você seleciona [TLS], é necessário instalar o "Certificado de cliente IEEE 802.1X".
- Execute as seguintes definições de acordo com o sistema operacional a ser utilizado:
  - Selecione [Ligado] ou [Desligado] em "Autenticar certificado do servidor".
  - Selecione [Ligado] ou [Desligado] em "Confiar na autoridade de certificação intermediária".
  - Insira o nome de host do servidor RADIUS em "ID do servidor".
  - Selecione [Ligado] ou [Desligado] em "Permitir subdomínio".

7. **Clique em [OK].**
8. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
9. **Clique em [Definições da interface] em "Interface".**

10. Selecione [Ativo] em "Segurança da Ethernet".

11. Clique em [OK].

12. É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].

Se a tela anterior não reaparecer depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.

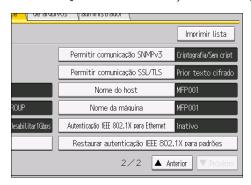
13. Faça logout.

- Se ocorrer um problema com as definições, talvez você não consiga se comunicar com o equipamento. Nesse caso, acesse [Imprimir lista] em [Definições da interface] no painel de controle e, em seguida, imprima o resumo da rede para verificar o status.
- Se não conseguir identificar o problema, execute [Restaurar autenticação IEEE 802.1X para padrões] em [Rede] em [Definições da interface] no painel de controle e, em seguida, repita o procedimento.

Criptografia SNMPv3

Ao utilizar o Device Manager NX ou outro aplicativo que se comunique via SNMPv3, você pode criptografar os dados transmitidos.

Efetuando esta definição, você pode impedir que os dados sejam adulterados.

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Definições de interface].**
4. **Pressione [▼Próximo].**
5. **Pressione [Permitir comunicação SNMPv3].**

6. **Pressione [Somente criptografia].**
7. **Pressione [OK].**
8. **Faça logout.**

- Para utilizar o Device Manager NX para criptografar os dados de especificação de definições, é necessário especificar a definição [Senha de criptografia] do administrador de rede e [Encrypted Password] (Senha criptografada) em [SNMP Account Setting] (Definição de conta SNMP) em Device Manager NX, além de especificar [Permitir comunicação SNMPv3] no equipamento. Para obter detalhes sobre a especificação da [Encrypted Password] (Senha criptografada) em Device Manager NX, consulte a Ajuda do Device Manager NX.
- Se a definição da [Senha de criptografia] do administrador da rede não estiver especificada, os dados para transmissão podem não ser criptografados ou enviados. Para informações sobre como especificar a definição da [Senha de criptografia] do administrador da rede, consulte Pág. 17 "Registro e alteração de administradores".

Criptografar Senhas transmitidas

A configuração da chave de criptografia do driver e da criptografia de senha para a Autenticação IPP ativa a comunicação com senhas criptografadas e aumenta a segurança contra quebra de senhas. Para aumentar ainda mais a segurança, recomendamos o uso combinado de IPsec, SNMPv3 e SSL/ TLS.

Criptografe também a senha de login para autenticação do administrador e dos usuários.

Chave de criptografia de driver

Essa chave é uma sequência de caracteres utilizada para criptografar senhas de login ou senhas de documentos enviadas de cada driver quando a autenticação do usuário estiver ativada.

Para criptografar a senha de login, especifique a chave de criptografia do driver no equipamento e no driver de impressão instalado no computador do usuário.

Senha para Autenticação IPP

Para criptografar a senha de Autenticação IPP no Web Image Monitor, defina "Autenticação" como [DIGEST] e especifique a senha de Autenticação IPP no equipamento.

Você pode utilizar telnet ou FTP para gerenciar senhas para a autenticação IPP, embora não seja recomendado.

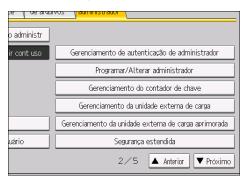
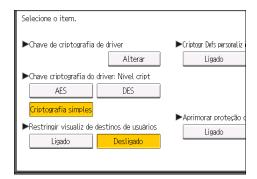
- Para obter detalhes sobre criptografia das senhas de login usadas na autenticação de administrador, consulte Pág. 17 "Registro e alteração de administradores".

Especificar uma chave de criptografia de driver

Especifique a chave de criptografia do driver no equipamento.

Essa definição ativa a transmissão criptografada de senhas de login e aumenta a segurança contra quebra de senhas.

1. **Faça login como administrador de rede no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**

5. **Pressione [Segurança estendida].**

6. **Para "Chave de criptografia de driver", pressione [Alterar].**

7. **Insira a chave de criptografia do driver e, em seguida, pressione [OK].**

   Insira a chave de criptografia do driver utilizando até 32 caracteres alfanuméricos.

   O administrador da rede deve fornecer aos usuários a chave de criptografia especificada no equipamento para que eles possam registrá-la em seus computadores. Certifique-se de inserir a mesma chave de criptografia de driver especificada no equipamento.

8. **Pressione [OK].**
9. **Faça logout.**

- Para mais informações sobre como especificar a chave de criptografia no driver de impressão ou TWAIN, consulte a ajuda do driver.

Especificar uma senha de Autenticação IPP

Especificar uma senha de Autenticação IPP para este equipamento. Essa definição ativa a transmissão criptografada de senhas de autenticação IPP e aumenta a segurança contra a quebra de senhas.

1. **Faça login como administrador da rede no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**

3. **Clique em [Autenticação IPP] em "Segurança".**
4. **Selecione [DIGEST] da lista "Autenticação".**
5. **Insira o nome de usuário na caixa "Nome de usuário".**
6. **Insira a senha na caixa "Senha".**
7. **Clique em [OK].**

   A Autenticação IPP é especificada.
8. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
9. **Faça logout.**

Definições de criptografia da autenticação Kerberos

É possível especificar transmissões criptografadas entre o equipamento e o centro de distribuição de chave (KDC) quando a autenticação Kerberos está ativada.

O uso da autenticação Kerberos com o Windows ou a autenticação LDAP, pesquisa LDAP, etc., assegura uma comunicação segura.

O algoritmo de criptografia suportado varia dependendo do tipo de servidor KDC. Selecione o algoritmo mais adequado para o seu ambiente.

Servidor KDC	Algoritmos de criptografia suportados
Windows Server 2003 Active Directory	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* Para usar a autenticação Kerberos, ative-a nas definições do sistema operacional.

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Autenticação Kerberos] em "Definições do dispositivo".**
4. **Selecione o algoritmo de criptografia que deseja ativar.**

   Selecione um ou mais algoritmos de criptografia.

5. **Clique em [OK].**
6. **Faça logout.**

6. Evitar vazamentos de documentos

Este capítulo descreve como proteger dados de documentos armazenados no equipamento ou impressos usando o equipamento.

Gerenciar pastas

Esta seção explica como gerenciar as pastas no Servidor de documentos, como excluir pastas, alterar senhas e desbloqueá-las quando bloqueadas.

Excluir pastas

Isto pode ser feito pelo administrador de arquivo ou por um usuário.

Para excluir uma pasta com o ícone , é necessária a senha da pasta.

Se um usuário esquecer a senha de acesso à pasta, o administrador de arquivo poderá alterá-la.

O administrador de arquivo pode excluir pastas sem utilizar a senha.

As pastas contendo arquivos para os quais o usuário não tem permissão para excluir não podem ser excluídas.

A pasta compartilhada não pode ser excluída.

1. **Faça login como administrador de arquivo ou como usuário do painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

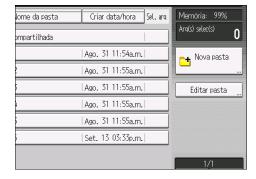
   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

6

CWW220

4. **Pressione [Editar pasta].**

5. **Selecione a pasta.**
6. **Pressione [Excluir].**
7. **Se uma tela de entrada de senha aparecer, insira a senha da pasta e pressione [OK].**

   A tela de inserção de senha não aparecerá se o administrador de arquivo tiver feito login.
8. **Pressione [Excluir].**
9. **Faça logout.**

Nota

- Este procedimento também pode ser feito no Web Image Monitor. Para obter detalhes, consulte a Ajuda do Web Image Monitor.

Alterar a senha de uma pasta

Esta opção pode ser especificada pelo administrador de arquivo ou por um usuário.

Se um usuário esquecer a senha de acesso à pasta, o administrador de arquivo poderá alterá-la.

Não é possível especificar uma senha para a pasta compartilhada.

1. **Faça login como administrador de arquivo ou como usuário do painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
4. **Pressione [Editar pasta].**

5. **Selecione a pasta.**
6. **Pressione [Alterar senha].**
7. **Se uma tela de entrada de senha aparecer, insira a senha da pasta e pressione [OK].**

   A tela de inserção de senha não aparecerá se o administrador de arquivo tiver feito login.
8. **Insira a nova senha para a pasta e pressione [OK].**

   Você pode usar de 4 a 8 números como senha para a pasta.
9. **Insira a senha para confirmação novamente e pressione [OK].**

   O ícone aparece próximo a uma pasta protegida por senha.
10. **Faça logout.**

- Este procedimento também pode ser feito no Web Image Monitor. Para obter detalhes, consulte a Ajuda do Web Image Monitor.

Desbloquear pastas

Apenas o administrador de arquivo pode desbloquear pastas.

Se você especificar [Ligado] para "Aprimorar proteção de arquivo", a pasta será bloqueada e ficará inacessível se uma senha inválida for inserida 10 vezes. Este capítulo explica como desbloquear pastas.

"Aprimorar proteção de arquivo" é uma das funções de segurança estendidas. Para detalhes sobre esta e outras funções de segurança estendida, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

1. **Faça login como administrador de arquivo no painel de controle.**
2. **Pressione a tecla [User Tools].**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
4. **Pressione [Editar pasta].**
5. **Selecione a pasta.**

   O ícone aparece próximo a uma pasta bloqueada pela função Aprimorar proteção de arquivo.
6. **Pressione [Desbloquear].**

   O ícone é alterado para o ícone .
7. **Pressione [Desbloquear].**
8. **Faça logout.**

- Este procedimento também pode ser feito no Web Image Monitor. Para obter detalhes, consulte a Ajuda do Web Image Monitor.

Gerenciar arquivos armazenados

Esta seção descreve como especificar as permissões de acesso a arquivos armazenados.

Você pode especificar a quem é permitido o acesso a arquivos digitalizados armazenados no Servidor de documentos.

Isso evita atividades como impressão ou envio de arquivos armazenados por usuários não autorizados.

Você também pode especificar que usuários podem alterar ou excluir arquivos armazenados.

Para limitar a utilização de arquivos armazenados, você pode especificar 4 tipos de permissão de acesso.

Tipos de permissão de acesso

Permissão de acesso	Descrição
Somente leitura	É possível verificar o conteúdo e a informação dos arquivos armazenados, imprimir e enviar os arquivos.
Editar	Você pode alterar as definições de impressão para arquivos armazenados. Isto inclui permissão para visualizar arquivos.
Editar/Excluir	Você pode excluir arquivos armazenados. Isto inclui permissão para visualizar e editar arquivos.
Controle total	Pode especificar o usuário e a permissão de acesso. Isto inclui permissão para visualizar, editar e editar/excluir arquivos.

Senha para arquivos armazenados

- As senhas para os arquivos armazenados podem ser especificadas pelo administrador ou proprietário.
  É possível aumentar a proteção contra a utilização não autorizada de arquivos. Para detalhes sobre atribuição de uma senha a um arquivo armazenado, consulte Pág. 177 "Especificar senhas para arquivos armazenados".
- Mesmo que a autenticação de utilizador não esteja definida, podem ser definidas palavras-passe para os ficheiros guardados.

- Os arquivos podem ser armazenados por qualquer usuário com permissão para usar a função de Servidor de documentos, cópia, scanner ou impressão.
- Utilizando o Web Image Monitor, você pode verificar o conteúdo de arquivos armazenados. Para mais informações, consulte a Ajuda do Web Image Monitor.

- A permissão de acesso padrão para o proprietário é "Somente leitura".

  Você também pode especificar a permissão de acesso.
- O administrador de arquivo não apenas configura as permissões de acesso, mas também pode excluir arquivos armazenados. Para mais informações sobre métodos de exclusão de documentos, consulte Copy/ Document Server.

Configurar permissão de acesso para cada arquivo armazenado

Esta opção pode ser especificada pelo administrador de arquivo ou proprietário.

Especifique usuários e suas permissões de acesso para cada arquivo armazenado.

- Se os arquivos se tornarem inacessíveis, redefina a permissão de acesso como proprietário.

  O administrador de arquivo pode redefinir a permissão de acesso. Se você deseja acessar um arquivo, mas não tem permissão de acesso, solicite ao proprietário.

- O administrador de arquivos pode alterar o proprietário de um documento utilizando a definição [Alt.priv. de acesso]. Esta definição permite também ao administrador de arquivo alterar os privilégios de acesso do proprietário e outros usuários.
- O proprietário do documento e os usuários com o privilégio [Controle total] sobre o documento podem alterar os privilégios de acesso do proprietário e de outros usuários na definição [Alt. priv. de acesso].

1. **Efetue login como administrador de arquivos ou como proprietário no painel de controle.**

2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

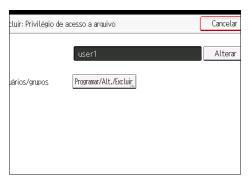
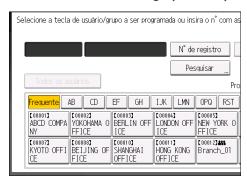
   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

4. **Selecione a pasta.**

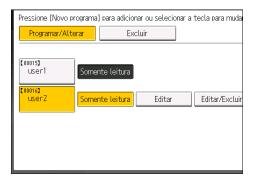
5. **Selecione o arquivo.**

6. **Pressione [Editar arquivo].**

6

7. **Pressione [Alt. priv. de acesso].**
8. **Pressione [Programar/Alterar/Excluir].**

9. **Pressione [Novo progr].**
10. **Selecione os usuários ou grupos aos quais deseja atribuir permissões de acesso.**

É possível selecionar usuários múltiplos.

Pressione [Todos usuários] para selecionar todos os usuários.

11. **Pressione [Sair].**
12. **Selecione o usuário a quem deseja atribuir uma permissão de acesso, selecionando, em seguida, a permissão.**

Selecione a permissão de acesso em [Somente leitura], [Editar], [Editar/Excluir] ou [Controle total].

13. **Pressione [Sair].**
14. **Pressione [OK].**
15. **Faça logout.**

- Este procedimento também pode ser feito no Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- As permissões de acesso "Editar", "Editar/Excluir" e "Controle total" permitem ao usuário executar operações de alto nível que podem resultar na perda ou em alterações de informações importantes. Recomendamos que você atribua apenas a permissão "Somente leitura" a usuários gerais.

Alterar o proprietário de um documento

Utilize este procedimento para alterar o proprietário de um documento.

Apenas o administrador de arquivo pode alterar o proprietário de um documento.

1. **Faça login como administrador de arquivo no painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
4. **Selecione a pasta.**
5. **Selecione o arquivo.**
6. **Pressione [Editar arquivo].**
7. **Pressione [Alt. priv. de acesso].**
8. **Pressione [Alterar] para "Proprietário".**
9. **Selecione o usuário que deseja registrar.**
10. **Pressione [Sair].**
11. **Pressione [OK].**
12. **Faça logout.**

Configurar permissão de acesso para cada usuário de arquivos armazenados

Isso pode ser especificado pelo administrador de usuários ou proprietário.

Especifique usuários e suas permissões de acesso a arquivos armazenados por um determinado usuário.

Isto torna o gerenciamento da permissão de acesso mais fácil do que especificar e gerenciar permissões de acesso para cada arquivo armazenado.

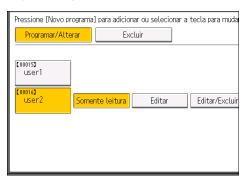
- Se os arquivos não forem acessíveis, peça ao administrador de usuário para redefinir as permissões de acesso aos arquivos.

1. **O administrador de usuários ou o proprietário faz login no painel de controle.**
2. **Pressione [Gerenc. Catálogo de end].**
3. **Selecione o usuário.**
4. **Pressione [Proteção].**
5. **Em "Proteger arquivo(s)", pressione [Programar/Alterar/Excluir] para "Permissões para usuários/grupos".**

6. **Pressione [Novo progr].**
7. **Selecione os usuários ou grupos a serem registrados.**

   É possível selecionar usuários múltiplos.

   Pressione [Todos usuários] para selecionar todos os usuários.
8. **Pressione [Sair].**

9. **Selecione o usuário a quem deseja atribuir uma permissão de acesso, selecionando, em seguida, a permissão.**

Selecione a permissão de acesso em [Somente leitura], [Editar], [Editar/Excluir] ou [Controle total].

10. **Pressione [Sair].**
11. **Pressione [OK].**
12. **Pressione [Sair].**
13. **Faça logout.**

- As permissões de acesso "Editar", "Editar/Excluir" e "Controle total" permitem ao usuário executar operações de alto nível que podem resultar na perda ou em alterações de informações importantes. Recomendamos que você atribua apenas a permissão "Somente leitura" a usuários gerais.

Especificar senhas para arquivos armazenados

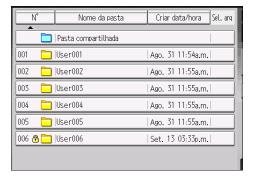
Esta opção pode ser especificada pelo administrador de arquivo ou proprietário.

1. **O administrador de arquivo ou o proprietário faz login no painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

4. **Selecione a pasta.**

5. **Selecione o arquivo.**

6. **Pressione [Editar arquivo].**

7. **Pressione [Alterar senha].**
8. **Insira a nova senha para o arquivo armazenado e pressione [OK].**

   Você pode usar de 4 a 8 números como senha para o arquivo armazenado.

9. **Reinsira a senha para confirmação e pressione [OK].**

   O ícone aparece ao lado de um arquivo armazenado protegido por senha.

10. **Pressione [OK].**
11. **Faça logout.**

Desbloquear arquivos armazenados

Apenas o administrador de arquivos pode desbloquear arquivos.

Se você especificar "Aprimorar proteção de arquivo", o arquivo será bloqueado e ficará inacessível caso uma senha inválida seja inserida 10 vezes. Este capítulo explica como desbloquear arquivos.

"Aprimorar proteção de arquivo" é uma das funções de segurança estendidas. Para obter mais informações sobre esta e outras funções de segurança estendidas, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

1. **Faça login como administrador de arquivo no painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

3. **Pressione a tecla [Tela inicial] no painel de controle e pressione o ícone [Servidor de documentos] na tela.**

   Se o ícone [Servidor de documentos] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

4. **Selecione a pasta.**
5. **Selecione o arquivo.**

   O ícone aparece ao lado de um arquivo bloqueado pela função Aprimorar proteção de arquivo.

6. **Pressione [Editar arquivo].**

7. **Pressione [Desbloq arquivos].**

8. **Pressione [Sim].**

   O ícone é alterado para o ícone .

9. **Pressione [OK].**

10. **Faça logout.**

6

Gerenciar arquivos de impressão bloqueada

Dependendo da localização do equipamento, pode ser difícil evitar que pessoas não autorizadas vejam as impressões carregadas nas bandejas de saída. Ao imprimir documentos confidenciais, utilize a função Impressão bloqueada.

Impressão bloqueada

- Use a função Impressão bloqueada para armazenar arquivos no equipamento como arquivos de Impressão bloqueada. Imprima os arquivos no painel de controle e recupere-os imediatamente para que os outros não os vejam.

- É possível imprimir documentos confidenciais independentemente das definições de autenticação de usuário.
- Para armazenar arquivos temporariamente, selecione [Impressão armazenada] no driver de impressão. Se você selecionar [Impressão armaz. (compartilhada)], também poderá compartilhar estes arquivos.
- Para mais informações sobre como usar a função Impressão bloqueada, consulte Impressão.

Excluir arquivos de impressão bloqueada

Esta opção pode ser especificada pelo administrador de arquivo ou proprietário.

Para que o proprietário possa excluir um arquivo de Impressão bloqueada, é necessária a senha para acessar o arquivo.

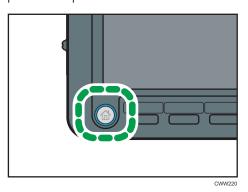
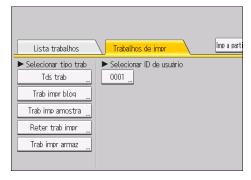
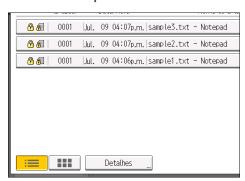
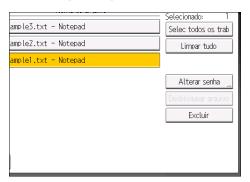
Caso o proprietário tenha se esquecido da senha, o administrador de arquivos pode alterá-la.

A senha não é necessária para que o administrador de arquivos exclua os arquivos de Impressão bloqueada.

1. **Efetue login como administrador de arquivos ou como proprietário no painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

3. **Pressione a tecla [Tela inicial] no painel de controle e clique no ícone [Impressora] na tela.**

   Se o ícone [Impressora] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

4. **Pressione [Trabs impr].**
5. **Pressione [Trab impr bloq].**

6. **Selecione o arquivo.**

7. **Pressione [Excluir].**

8. **Se uma tela de entrada de senha aparecer, insira a senha do arquivo de impressão bloqueado e pressione [OK].**

   A tela de inserção de senha não aparecerá se o administrador de arquivo tiver feito login.

9. **Pressione [Sim].**
10. **Faça logout.**

- Você pode configurar este equipamento para excluir automaticamente arquivos armazenados definindo a opção Excluir autom os trab de imp como [Ligado]. Para obter mais informações sobre "Excluir autom os trab de imp temp", consulte "Imprimir.

- Este procedimento também pode ser feito no Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Alterar a senha de um arquivo de impressão bloqueada

Esta opção pode ser especificada pelo administrador de arquivo ou proprietário.

Caso o proprietário tenha se esquecido da senha, o administrador de arquivos pode alterá-la.

1. **Efetue login como administrador de arquivos ou como proprietário no painel de controle.**

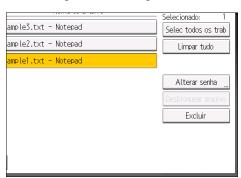
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].

3. **Pressione a tecla [Tela inicial] no painel de controle e clique no ícone [Impressora] na tela.**

   Se o ícone [Impressora] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.

4. **Pressione [Trabs impr].**
5. **Pressione [Trab impr bloq].**

6. **Selecione o arquivo.**
7. **Pressione [Alterar senha].**

8. **Se uma tela de entrada de senha aparecer, insira a senha para o arquivo armazenado e pressione [OK].**

   A tela de inserção de senha não aparecerá se o administrador de arquivos tiver feito login.

9. **Insira a nova senha para o arquivo armazenado e pressione [OK].**
10. **Insira a senha para confirmação novamente e pressione [OK].**
11. **Faça logout.**

- Este procedimento também pode ser feito no Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Desbloquear um arquivo de impressão bloqueada

Apenas o administrador de arquivos pode desbloquear arquivos.

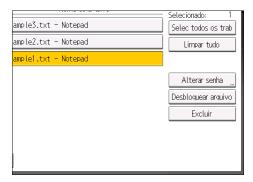
Se você especificar [Ligado] para "Aprimorar proteção de arquivo", o arquivo será bloqueado e ficará inacessível se uma senha inválida for inserida 10 vezes. Este capítulo explica como desbloquear arquivos.

"Aprimorar proteção de arquivo" é uma das funções de segurança estendidas. Para obter mais informações sobre esta e outras funções de segurança estendidas, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".

1. **Faça login como administrador de arquivo no painel de controle.**
2. **Pressione a tecla [Ferramentas] para fechar o menu Ferramentas.**

   Se a mensagem "Você não tem os privilégios necessários para usar essa função." aparecer, pressione [Sair].
3. **Pressione a tecla [Tela inicial] no painel de controle e clique no ícone [Impressora] na tela.**

   Se o ícone [Impressora] não for exibido, pressione o ícone no canto superior direito da tela para mudar para a tela do menu.
4. **Pressione [Trabs impr].**
5. **Pressione [Trab impr bloq].**
6. **Selecione o arquivo.**

   O ícone aparece ao lado de um arquivo bloqueado pela função Aprimorar proteção de arquivo.
7. **Pressione [Desbloq arq].**

8. **Pressione [Sim].**

   O ícone desaparece.
9. **Faça logout.**

6

- Este procedimento também pode ser feito no Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.

Prevenção contra cópia não autorizada / Segurança de dados para cópia

A função da impressora permite a integração de um padrão em uma cópia impressa para desincentivar ou evitar cópia não autorizada.

Se a função Prevenção contra cópia não autorizada estiver ativada, padrões de textos incorporados (por exemplo, uma mensagem de aviso como "Não é permitido copiar") são exibidos quando os documentos são copiados ilegalmente.
Dessa forma, cópias não autorizadas podem ser evitadas.

Se a função Segurança de dados para cópia estiver sendo utilizada e as definições para padrões especiais incorporados em documentos estiverem ativadas, cópias de documentos com padrões incorporados são sobreimpressos em cinza.

Dessa forma, o vazamento de informações pode ser evitado. Para proteger documentos com sobreimpressão cinza, a copiadora ou impressora multifuncional deve ser instalada com Copy Data Security Unit.

Para obter mais detalhes, consulte as informações abaixo:

Utilizar a prevenção contra cópia não autorizada

1. Ativar impressão do padrão integrado. O administrador da máquina configura esta configuração. Para informações sobre como configurar as definições, consulte Pág. 188 "Ativar a impressão de padrões".
2. Especifique as configurações para a prevenção de cópia não autorizada na função da impressora. O privilégio para especificar a definição depende da definição especificada em [Prevenção contra cópia não autorizada obrigat].

   Para mais informações, consulte Pág. 188 "Ativar a impressão de padrões".

Utilizar a Segurança de dados para cópia

1. Ativar a configuração de impressão de padrão integrado. O administrador da máquina configura esta configuração. Para informações sobre como configurar as definições, consulte Pág. 188 "Ativar a impressão de padrões".
2. Especificar as configurações de segurança de dados para cópia na função de impressora. O privilégio para especificar a definição depende da definição especificada em [Prevenção contra cópia não autorizada obrigat].

   Para mais informações, consulte Pág. 188 "Ativar a impressão de padrões".

Ativar a impressão de padrões

É possível ativar a impressão de padrão incorporado para desestimular ou impedir a cópia não autorizada.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Impr c/prev contra cópia não autor: Impressora].**
6. **Pressione [Alterar] para "Def de prev contra cópia não autoriz".**
7. **Pressione [Ligado] e, em seguida, [OK].**
8. **Pressione [Alterar] para "Prevenção contra cópia não autorizada obrigat".**
9. **Especifique se deseja ou não definir como obrigatória a impressão do padrão incorporado.**
    - [Driver/Comando]

      A impressão do padrão incorporado não é obrigatória.

      Ao utilizar o driver de impressão, os usuários podem optar pela impressão com o padrão incorporado e podem especificar suas definições.

    - [Driver/Comando(maioria defs)]

      A impressão do padrão incorporado é obrigatória.

      Ao utilizar o driver de impressão, os usuários podem especificar as definições de padrão incorporado com exceção de tipo, cor e espessura.

    - [Defin da máquina]

      A impressão do padrão incorporado é obrigatória.

      Os usuários não podem especificar as definições de padrão incorporado utilizando o driver de impressão.
10. **Pressione [OK] duas vezes.**
11. **Faça logout.**

- Para mais informações sobre as definições para especificar o padrão utilizando o equipamento, consulte Connecting the Machine/ System Settings.

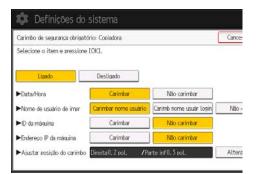
Imprimir informações do usuário em papel

A hora de início do trabalho de impressão, informações sobre a pessoa que o imprime (nome ou nome de usuário de login), número do equipamento e o endereço IP do equipamento podem ser obrigatoriamente incorporados em folhas impressas. Esta função é chamada de Carimbo de segurança obrigatório.

A impressão das informações sobre a pessoa que está imprimindo o trabalho pode desestimular o vazamento de informações. Essa opção também pode ser usada para identificar as origens do vazamento de informações.

O carimbo de segurança obrigatório pode ser usado com as funções de cópia, Servidor de documentos e impressora.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Selecione a(s) função(s) para o Carimbo de segurança obrigatório.**
    - Para definir o carimbo de segurança obrigatório para a função de cópia, pressione [Carimbo de segurança obrig: Copiadora].
    - Para definir o Servidor de documentos a ser carimbado, pressione [Carimbo de segurança obrig:serv doc.].
    - Para definir o carimbo de segurança obrigatório para a função de impressora, pressione [Carimbo de segurança obrig: Impress].
6. **Pressione [Ligado], e, em seguida, selecione os dados a serem marcados com o carimbo.**

    Para desativar a função de carimbo de segurança obrigatório, pressione [Desligado].

- Data/Hora

    A hora de início do trabalho será impressa.

- Nome de usuário de impr

Essas informações serão impressas se a autenticação de usuário estiver habilitada.

- Carimbar nome usuário

  O "Nome" em "Nomes" no Catálogo de endereços será impresso.

- Carimb nome usuár login

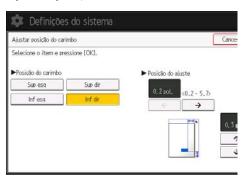
  O código de usuário ou o nome de usuário de login em "Inform Aut." no Catálogo de endereços será impresso.

- ID da máquina

  Os números exibidos como o "Número de série do equipamento" em [Consulta] será impresso.

- Endereço IP da máquina

  O endereço IP do equipamento será impresso. Se houver endereços IPv4 e IPv6, o endereço IPv4 será impresso. Se nenhum endereço IP tiver sido configurado, essa informação ficará em branco.

7. **Pressione [Alterar] para "Ajustar posição do carimbo".**
8. **Ajuste a posição do carimbo.**

9. **Pressione [OK] duas vezes.**
10. **Faça logout.**

Armazenagem imposta de documentos a serem impressos em uma impressora

Ao tornar obrigatório o armazenamento dos trabalhos no equipamento antes de imprimi-los, você pode impedir o vazamento de informações caso você não colete as impressões ou deixe o equipamento sozinho. Os seguintes trabalhos de impressão estão sujeitos ao armazenamento obrigatório.

- Impressão normal
- Impressão de teste
- Armazenar e imprimir

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Recursos da impr].**
3. **Pressione [Sistema].**
4. **Pressione [▼Próximo].**
5. **Pressione [Restringir trabs de impr direta].**
6. **Pressione [Armazenar trabs aut].**
7. **Pressione [OK].**
8. **Faça logout.**

- Se você selecionar [Canc tds trabs imp dir], os trabalhos de impressão serão cancelados sem que sejam armazenados.
- Para informação sobre como imprimir documentos armazenados, consulte "Imprimir documentos armazenados", Impressão.

7. Gerenciar o equipamento

Este capítulo descreve as funções para aprimorar a segurança do equipamento e utilizá-lo de modo eficiente

Gerenciar arquivos de log

A coleta de logs armazenados no equipamento permite rastrear dados detalhados sobre acessos ao equipamento, identidades de usuários, uso das várias funções do equipamento e históricos de erros.

Os logs podem ser excluídos periodicamente para disponibilizar espaço em disco.

Os logs podem ser exibidos usando o Web Image Monitor ou o servidor de coleta de logs. Os logs coletados podem ser convertidos em arquivos CSV e baixados de uma vez. Os logs coletados não podem ser lidos diretamente do disco rígido.

Tipos de log

Três tipos de log são armazenados no equipamento: o log de trabalhos, o log de acessos e o log ecológico.

- Log de trabalhos

  Armazena detalhes de operações relacionadas ao arquivo do usuário, como cópia, impressão e salvamento no Servidor de documentos e de operações do painel de controle, como envio de arquivos digitalizados e relatórios de impressão (a lista de configurações, por exemplo).

- Log de acessos

  Armazena detalhes de atividades de login e logout, operações com arquivos armazenados, como criação, edição e exclusão; operações de técnicos do cliente, como formatação do disco rígido; operações do sistema, como visualização dos resultados de transferências de logs e operações de segurança, como especificação de definições de criptografia, detecção de acessos não autorizados, bloqueio de usuários e autenticação de firmware.

- Log ecológico

  Armazena informações do Equipamento LIGADO, DESLIGADO, mudança no status da alimentação, tempos de execução de trabalhos ou intervalo de tempo entre trabalhos, consumo de papel por hora, consumo de energia.

- Para obter detalhes sobre o servidor de coleta de log, consulte o manual do usuário do servidor de coleta de log.
- Ao utilizar o servidor de coleta de logs, você deve configurar as transferências de logs no servidor de coleta de logs.

Utilizar o Web Image Monitor para gerenciar arquivos de log

Você pode especificar os tipos de log a serem armazenados no equipamento e o nível de coleta de logs. Também pode excluir em massa ou baixar arquivos de log.

Logs que podem ser gerenciados usando o Web Image Monitor

As tabelas a seguir explicam os itens no log de trabalhos e log de acessos que o equipamento cria quando você ativa a coleta de logs usando o Web Image Monitor. Caso precise coletar logs, utilize o Web Image Monitor para configurá-lo. Esta definição pode ser especificada em [Logs] na opção [Configuração] no Web Image Monitor.

Itens das informações de log de trabalhos

Item de log de trabalhos	Atributo do tipo de log	Conteúdo
Copiadora: Copiando	Copier: Copying	Detalhes de trabalhos normais e de cópia de teste.
Copiadora: Copiando e armazenando	Copier: Copying and Storing	Detalhes dos arquivos armazenados no Servidor de documentos que também foram copiados no momento do armazenamento.
Servidor de documentos: Armazenando	Document Server: Storing	Detalhes dos arquivos armazenados usando a tela Servidor de documentos.
Servidor de documentos: Download de arquivo armazenado	Document Server: Stored File Downloading	Detalhes dos arquivos armazenados no Servidor de documentos e baixados utilizando o Web Image Monitor.
Utility: Storing	Utility: Storing	Informações detalhadas dos arquivos armazenados que usam um utilitário.
Impressão de arquivo armazenado	Stored File Printing	Detalhes dos arquivos impressos usando a tela Servidor de documentos.
Scanner: Enviando	Scanner: Sending	Detalhes dos arquivos de digitalização enviados.

Item de log de trabalhos	Atributo do tipo de log	Conteúdo
Scanner: Envio e armazenamento de link de URL	Scanner: URL Link Sending and Storing	Detalhes dos arquivos de digitalização armazenados no Servidor de documentos. Os URLs foram enviados por e-mail na ocasião do armazenamento.
Scanner: Enviando e armazenando	Scanner: Sending and Storing	Detalhes dos arquivos de digitalização armazenados no Servidor de documentos que também foram enviados no momento do armazenamento.
Scanner: Armazenando	Scanner: Storing	Detalhes dos arquivos de digitalização armazenados no Servidor de documentos.
Scanner: Download de arquivo armazenado	Scanner: Stored File Downloading	Detalhes dos arquivos de digitalização armazenados no Servidor de documentos e baixados utilizando o Web Image Monitor ou o Desk Top Editor For Production.
Scanner: Envio de arquivo armazenado	Scanner: Stored File Sending	Detalhes dos arquivos de digitalização armazenados que também foram enviados.
Scanner: Envio de link de URL de arquivo armazenado	Scanner: Stored File URL Link Sending	Detalhes dos arquivos de digitalização armazenados cujas URLs foram enviadas por e-mail.
Impressora: Imprimindo	Printer: Printing	Detalhes dos trabalhos de impressão normais.
Impressora: Impressão bloqueada (Incompleta)	Printer: Locked Print (Incomplete)	Log mostrando documentos de Impressão bloqueada armazenados temporariamente no equipamento.
Impressora: Impressão bloqueada	Printer: Locked Print	Log mostrando documentos de Impressão bloqueada armazenados temporariamente no equipamento e impressos a partir do painel de controle ou através do Web Image Monitor.
Impressora: Impressão de teste (Incompleto)	Printer: Sample Print (Incomplete)	Log mostrando documentos de Impressão de teste armazenados temporariamente no equipamento.

Item de log de trabalhos	Atributo do tipo de log	Conteúdo
Impressora: Impressão de teste	Printer: Sample Print	Log mostrando documentos de Impressão de teste armazenados temporariamente no equipamento e impressos a partir do painel de controle ou através do Web Image Monitor.
Impressora: Reter impressão (Incompleta)	Printer: Hold Print (Incomplete)	Log mostrando documentos de Reter impressão armazenados temporariamente no equipamento.
Impressora: Reter impressão	Printer: Hold Print	Log mostrando documentos de Reter impressão armazenados temporariamente no equipamento e impressos a partir do painel de controle ou através do Web Image Monitor.
Impressora: Impressão armazenada	Printer: Stored Print	Detalhes de arquivos de Impressão armazenada armazenados no equipamento.
Impressora: Impressão armazenada e normal	Printer: Store and Normal Print	Detalhes dos arquivos de Impressão armazenada impressos no momento do armazenamento (quando "Tipo de trabalho:" estava definido como "Armazenar e imprimir" nas propriedades da impressora).
Impressora: Impressão de arquivo armazenado	Printer: Stored File Printing	Detalhes dos arquivos de Impressão armazenada impressos a partir do painel de controle ou através do Web Image Monitor.
Impressora: Envio de servidor de documentos	Printer: Document Server Sending	Detalhes dos arquivos armazenados no Servidor de documentos quando "Tipo trabalho:" estava definido como "Servidor de documentos nas propriedades da impressora.
Impressão de relatório	Report Printing	Detalhes dos relatórios impressos a partir do painel de controle.
Impressão/E-mail de relatório de resultados	Impressão/E-mail de relatório de resultados	Detalhes de resultados de trabalhos impressos a partir do painel de controle ou notificados por e-mail.

Item de log de trabalhos	Atributo do tipo de log	Conteúdo
Scanner: Leitura do driver TWAIN	Scanner: TWAIN Driver Scanning	Detalhes dos arquivos de digitalização armazenados que foram enviados utilizando o scanner TWAIN de rede.
Impressora: Reter impressão de arquivo	Printer: Hold Print File Printing	Quando um documento é retido para impressão e armazenado temporariamente no equipamento, é registrada a hora em que um usuário especifica a impressão do documento através do painel de controle ou do Web Image Monitor.

Itens de informações de log de acessos

Item de log de acessos	Atributo do tipo de log	Conteúdo
Login	Login	Horários de login e identidade de usuários que fizeram login.
Logout	Logout	Horários de logout e identidade de usuários que fizeram logout.
Armazenamento de arquivo	File Storing	Detalhes de arquivos armazenados no Servidor de documentos.
Exclusão de arquivo armazenado	Stored File Deletion	Detalhes de arquivos excluídos do Servidor de documentos.
Exclusão de todos os arquivos armazenados	All Stored Files Deletion	Detalhes de exclusões de todos os arquivos do Servidor de documentos.
Formato HDD	HDD Format	Detalhes da formatação do disco rígido.
Exclusão de todos os logs	All Logs Deletion	Detalhes de exclusões de todos os logs.
Alteração de definição de log	Log Setting Change	Detalhes de alterações feitas nas definições de log.
Transferir resultado de logs	Transferir resultado de logs	Log do resultado da transferência do log para Remote Communication Gate S.

Item de log de acessos	Atributo do tipo de log	Conteúdo
Alteração de item de coleta de log	Log Collection Item Change	Detalhes de alterações dos níveis de coleta de logs de trabalhos, níveis de coleta de logs de acesso e tipos de logs coletados.
Coletar logs de comunicação criptografados	Collect Encrypted Communication Logs	Log da transmissão criptografada entre o utilitário, Web Image Monitor ou dispositivos externos.
Violação de acesso	Access Violation	Detalhes de falhas de tentativas de acesso.
Bloqueio	Lockout	Detalhes da ativação do bloqueio.
Firmware: Atualização	Firmware: Update	Detalhes de atualizações de firmware.
Firmware: Alteração de estrutura	Firmware: Structure Change	Detalhes de alterações de estrutura que ocorreram quando foi inserido ou retirado um cartão SD ou inserido um cartão SD não suportado.
Firmware: Estrutura	Firmware: Structure	Detalhes de verificações de alterações na estrutura do módulo do firmware feitas, por exemplo, quando o equipamento foi ligado.
Alteração da chave de criptografia de dados da máquina	Machine Data Encryption Key Change	Detalhes das alterações feitas nas chaves de criptografia utilizando a definição "Alteração da chave de criptografia de dados da máquina".
Firmware: Inválido	Firmware: Invalid	Detalhes de verificações de validade do firmware feitas, por exemplo, quando o equipamento foi ligado.
Alteração de data/hora	Date/Time Change	Detalhes de alterações feitas nas definições de data e hora.
Alteração de privilégio de acesso ao arquivo	File Access Privilege Change	Log para alteração do privilégio de acesso aos arquivos armazenados.
Alteração de senha	Password Change	Detalhes de alterações feitas na senha de login.
Alteração de administrador	Administrator Change	Detalhes de alterações dos administradores.

Item de log de acessos	Atributo do tipo de log	Conteúdo
Alteração do catálogo de endereços	Address Book Change	Detalhes das alterações feitas nas entradas do Catálogo de endereços.
Configuração da máquina	Machine Configuration	Log de alterações nas definições do equipamento.
Fazer backup do Catálogo de endereços	Back Up Address Book	Log de quando é feito backup dos dados no Catálogo de endereços.
Restaurar Catálogo de endereços	Restore Address Book	Log de quando os dados no Catálogo de endereços são restaurados.
Limite de uso de volume de impr avançado: Resultado da permissão de rastreamento	Enhanced Print Volume Use Limitation: Tracking Permission Result	Log de quando ocorre um erro de rastreamento.
Resultado da limpeza do contador: Usuário(s) selecionado(s)	Counter Clear Result: Selected User(s)	Log de quando o contador de um dado usuário é limpo.
Resultado da limpeza do contador: Todos os usuários	Counter Clear Result: All Users	Log de quando os contadores de todos os usuários são limpos.
Importar informações de definição do dispositivo	Import Device Setting Information	Log de quando o arquivo de informações de definição do dispositivo é importado.
Exportar informações de definição do dispositivo	Export Device Setting Information	Log de quando o arquivo de informações de definição do dispositivo é exportado.
Criar/excluir pastas	Creating/Deleting Folders	Log de quando pastas são criadas e excluídas.
Edição de arquivo armazenado	Stored File Editing	Log para editar um arquivo.

Item de log de acessos	Atributo do tipo de log	Conteúdo
Inserção em outro arquivo	Inserção em outro arquivo	Log para inserir um arquivo em outro arquivo.

Não existe nenhum log de "Login" feito para SNMPv3.

Se o disco rígido for formatado, todas as entradas de log na ocasião da formatação são excluídas e é criada uma entrada de log indicando a conclusão da formatação.

"Violação de acesso" indica que o sistema tem sido alvo de frequentes ataques DoS remotos envolvendo tentativas de login através da autenticação de usuário.

O primeiro log criado após ligar é o log"Firmware: Estrutura".

Itens de informação de log ecológico

Item do log ecológico	Atributo do tipo de log	Conteúdo
Energia principal ligada	Main Power On	Log de quando o interruptor de energia principal é ligado.
Energia principal desligada	Main Power Off	Log de quando o interruptor de energia principal é desligado.
Resultado da transição do status de energia	Power Status Transition Result	Log dos resultados de transições do status de energia.
Informações relacionadas ao trabalho	Job Related Information	Log de informações relacionadas ao trabalho.
Uso de papel	Paper Usage	Log de quantidade de papel usado.
Consumo de energia	Power Consumption	Log de consumo de energia.

Atributos de logs que você pode baixar

Se você utilizar o Web Image Monitor para baixar logs, será criado um arquivo CSV com os itens de informações apresentados na tabela a seguir.

Observe que um campo em branco indica um item não incluído em um log.

Formato de saída do arquivo

- Conjunto de código de caracteres: UTF-8

- Formato de saída: CSV (Comma-Separated Values)
- Nomes de arquivos de logs de trabalhos e acessos: "nome do equipamento +_log.csv"
- Nomes de arquivos de logs ecológicos: "nome do equipamento +_ecolog.csv"

Ordem de entradas de log

As entradas de log são impressas em ordem crescente, de acordo com a ID do log.

Estrutura dos arquivos

O título dos dados é impresso na primeira linha (cabeçalho) do arquivo.

Diferenças de formatação de dados de logs

- Log de trabalhos

  Aparecem várias linhas na ordem de itens em comum (log de trabalhos e log de acessos), Origem (dados de entrada de trabalho) e Destino (dados de saída de trabalho).

  A ID do log atribuída é a mesma para todas as linhas correspondentes a uma entrada individual de log de trabalho.

	Start Date/Time	...	Result	...	Access Result	Source	...	Print File Name	Target	...	Stored File Name
1	20XX-12-03T15:43:03.0	...	Completed	...			...			...	
2		...	Completed	...		Report	...			...	
3		...	Completed	...			...		Print	...	

CJD022

1. **Itens em comum**

   Cada item nos itens em comum é exibido em uma linha separada.

2. **Origem**

   "Result" e "Status" aparecem nos itens em comum e na entrada de log de trabalhos.

   Se existirem várias origens, aparecerão várias linhas.

3. **Destino**

   "Result" e "Status" aparecerão nos itens em comum e na entrada de log de trabalhos.

   Se existirem vários destinos, aparecerão várias linhas.

- Log de acessos

  Os itens em comum e nas entradas do log de acessos aparecem em linhas separadas.

- Log ecológico

  As entradas de log ecológico aparecem em linhas separadas.

Itens em comum (log de trabalhos e log de acessos)

Start Date/Time

Indica a data e a hora de início de uma operação ou evento.

End Date/Time

Indica a data e a hora de término de uma operação ou evento.

Log Type

Detalhes do tipo de log.

Para detalhes sobre os itens de informações contidos em cada tipo de log, consulte Pág. 194 "Logs que podem ser gerenciados usando o Web Image Monitor".

Result

Indica o resultado de uma operação ou evento.

Os itens de log a seguir são registrados somente quando as operações registradas são executadas com sucesso:

"Document Server: Stored File Downloading", "Stored File Printing", "Scanner: Storing", "Scanner: Stored File Sending" e "Printer: Stored File Printing" (Logs de trabalhos) e "File Storing" e "Stored File Deletion" (Logs de acessos).

Valor	Conteúdo
Succeeded	A operação foi concluída com sucesso.
Failed	Ocorreu uma falha na operação ou evento.
<Em branco>	A operação ou evento ainda está em curso.

Operation Method

Indica o procedimento da operação.

Valor	Conteúdo
Control Panel	Painel de controle
Driver	Driver
Utility	Utilitário
Web	Web
Email	E-mail

Status

Indica o status de uma operação ou evento.

Valor	Conteúdo
Completed	A operação ou evento foi concluído com sucesso em uma entrada de trabalho.
Failed	Ocorreu uma falha na operação ou evento em uma entrada de trabalho.
Succeeded	A operação ou evento foi concluído com sucesso em uma entrada de log de acessos.
Password Mismatch	Ocorreu um erro devido a um erro de senha.
User Not Programmed	Ocorreu um erro de acesso, pois o usuário não é registrado.
Other Failures	Ocorreu um erro de acesso devido a uma falha não especificada.
User Locked Out	Ocorreu um erro de acesso, pois o usuário está bloqueado.
Communication Failure	Ocorreu um erro de acesso devido a uma falha de comunicação.
Communication Result Unknown	Ocorreu um erro de acesso devido a um resultado de comunicação desconhecido.
Failure in some or all parts	Ocorreu uma falha ao limpar o contador de usuário específico ou o contador de todos os usuários.
Importing/Exporting by Other User	A importação ou exportação está sendo executada por outro usuário.
Connection Failed with Remote Machine	Ocorreu uma falha na conexão com um destino de saída.
Write Error to Remote Machine	Ocorreu um erro ao gravar para um destino de saída.
Specified File: Incompatible	O arquivo especificado é incompatível.
Specified File: Format Error	Ocorreu um erro de formato com o arquivo especificado.
Specified File: Not Exist	O arquivo especificado não pode ser encontrado.
Specified File: No Privileges	O privilégio para acessar o arquivo especificado está ausente.
Specified File: Access Error	Ocorreu um erro ao acessar o arquivo especificado.
Memory Storage Device Full	O mídia externa está cheia.

Valor	Conteúdo
Memory Storage Device Error	Foi encontrada uma anormalidade na mídia externa.
Encryption Failed	Falha na criptografia.
Decoding Failed	Falha na decodificação.
Common Key Not Exist	A chave comum está ausente.
Connection Error	Ocorreu um erro de comunicação.
Specified Server Error	Ocorreu um erro de acesso, pois o servidor não está configurado corretamente.
Specified Client Error	Ocorreu um erro de acesso, pois o cliente não está configurado corretamente.
Authentication Settings Mismatch	As especificações do Catálogo de endereços não correspondem.
Authentication Method Mismatch	Os métodos de autenticação não correspondem.
Maximum Limit of Registered Number	O número máximo de equipamentos que podem ser registrados.
Invalid Password	A senha inserida não é válida.
Processing	O trabalho está sendo processado.
Error	Ocorreu um erro.
Suspended	O trabalho foi suspenso.

Cancelled: Details

Indica o estado em que a operação ou evento não obteve sucesso.

Valor	Conteúdo
Cancelled by User	Um usuário cancelou uma operação.
Input Failure	Uma entrada foi terminada inesperadamente.
Output Failure	Uma saída foi terminada anormalmente.
Other Error	Foi detectado um erro antes da execução de um trabalho ou ocorreram outros erros.

Valor	Conteúdo
Power Failure	Sem energia.
External Charge Unit Disconnected	O dispositivo de contabilidade foi desligado durante a operação.
Insufficient No. of Original for Overlay	Páginas faltando de um manuscrito durante a execução da cópia de overlaid.
Exceed Max. Stored Page (File Storage)	A capacidade de armazenamento de páginas no Servidor de documentos foi excedida.
Exceed Max. Stored File (File Storage)	A capacidade de armazenamento de documentos no Servidor de documentos foi excedida.
Hard Disk Full (File Storage Memory)	A capacidade do disco rígido no Servidor de documentos foi excedida.
Exceeded Max. Email Size	O limite de tamanho do e-mail foi excedido.
Exceeded Max. File Size	O limite de tamanho de um documento foi excedido.
Scanner Error	Ocorreu um erro de leitura com a alimentação automática de documentos.
Timeout	Tempo limite atingido.
Specified Folder to Store does not Exist	A pasta especificada para armazenar o arquivo não pode ser encontrada.
Password for Folder Specified to Store is Incorrect	A senha para a pasta especificada para armazenar o arquivo é incorreta.
Folder is Locked	A pasta está bloqueada.
Memory Full	A capacidade de memória para o processamento de dados está completa.
Print Data Error	Foi feita uma tentativa de usar um PDL ou uma porta não instalada no equipamento.
Data Transfer Interrupted	Casos devem ser registrados assim: • O driver usado não coincide. • Ocorreu um falha na rede.
Over Job Limit	O limite de trabalhos que podem ser recebidos foi excedido.

7

Valor	Conteúdo
Specifying Destination Error	Um endereço ilegal ou um endereço com 41 ou mais dígitos foi especificado.
Authentication Failed (Access Restricted)	Falha na autenticação do dispositivo.
Exceeded Print Volume Use Limitation	O limite de uso de papel para o usuário do login foi excedido.
No Privilege	O usuário não tem permissão para acessar um documento ou função.
Unavailable Size to Store	O tamanho do papel especificado (incluindo tamanhos personalizados) não pode ser armazenado.
Transmission Failed (Data Deleted)	Um documento foi excluído ou um documento que não foi enviado excedeu o tempo de espera e foi excluído.
Not Entered Document Password	A senha de um documento não foi inserida.
Connection Failed with Destination	O servidor ou pasta especificada não foi encontrada.
Authentication Failed with Destination	Falha na autenticação com o destino.
Transmission Failed with Memory Full	A memória de destino está cheia.
Invalid Device Certificate	Casos devem ser registrados assim: • O certificado do dispositivo está ausente. • O período válido expirou. • O endereço de e-mail do administrador e o do certificado não correspondem.
Invalid Expiration Date: Destination's Certificate	O período de validade do certificado de destino venceu.
Invalid Device/Destination's Certificate	O certificado de destino e o certificado de dispositivo são inválidos.
Book Function Error	Ocorreu um erro na função de encadernação.

Valor	Conteúdo
Fold Function Error	Ocorreu um erro na função de dobra.
Print Cancelled (Error)	O trabalho de impressão foi cancelado devido a um erro de sistema.

User Entry ID

Indica a ID de entrada do usuário.

Essa é uma ID hexadecimal que identifica usuários que executaram operações relacionadas a logs de trabalhos ou acessos.

Valor	Conteúdo
0x00000000	Operações de sistema, Operações que foram realizadas por usuários não autenticados
0x00000001 - 0xfffffeff	Para usuários gerais e código de usuário
0xffffff80	Operações de sistema
0xffffff81	Operações de sistema, Operações que foram realizadas por usuários não autenticados
0xffffff86	Supervisor
0xffffff87	Administrador
0xffffff88	Administrador 1
0xffffff89	Administrador 2
0xffffff8a	Administrador 3
0xffffff8b	Administrador 4

User Code/User Name

Identifica o código ou nome do usuário que executou a operação.

Se um administrador executou a operação, sua ID contém o nome de usuário de login do administrador.

Log ID

Identifica a ID atribuída ao log.

Essa é uma ID hexadecimal que identifica o log.

Itens de informações de log de acessos

Access Log Type

Indica o tipo de acesso.

Valor	Conteúdo
Authentication	Acesso de autenticação do usuário
Stored File	Acesso de arquivo armazenado
System	Acesso ao sistema
Network Attack Detection/ Encrypted Communication	Ataque de rede ou acesso de comunicação criptografado
Firmware	Acesso de verificação de firmware
Address Book	Acesso ao catálogo de endereços
Device Settings	Alterações realizadas em uma definição no menu Ferramentas do usuário.

Authentication Server Name

Indica o nome do servidor onde foi tentada a autenticação pela última vez.

No. of Authentication Server Switches

Indica o número de mudanças de servidor quando o servidor de autenticação não estava disponível.

Você pode verificar se o servidor de autenticação está disponível ou não.

O número de mudanças de servidor indicado é 0 a 4.

"0" indica que o servidor de autenticação está disponível.

Logout Mode

Modo de logout.

Valor	Conteúdo
by User's Operation	Logout manual feito pelo usuário
by Auto Logout Timer	Logout automático após tempo limite

Login Method

Indica a rota em que a solicitação de autenticação foi recebida.

Valor	Conteúdo
Control Panel	O login foi feito por meio do painel de controle.
via Network	O login foi feito remotamente através de um computador de rede.
Others	O login foi feito através de outro método.

Login User Type

Indica o tipo de usuário de login.

Valor	Conteúdo
User	Usuário geral
Guest	Usuário convidado
User Administrator	Administrador de usuário
Machine Administrator	Administrador de equipamento
Network Administrator	Administrador de redes
File Administrator	Administrador de arquivos
Supervisor	Supervisor
Customer Engineer (Service Mode)	Técnico do cliente
Others	Solicitações de usuários diferentes daqueles especificados acima

Target User Entry ID

Indica qual é a ID de entrada do usuário de destino.

Essa é uma ID hexadecimal que indica os usuários aos quais se aplicam as definições a seguir:

- Lockout
- Password Change

Target User Code/User Name

Código de usuário ou nome de usuário cujos dados foram acessados.

Se os dados do administrador foram acessados, é feito do login do nome de usuário do administrador.

Address Book Registration No.

Indica o número de registro do usuário realizando a operação.

Address Book Operation Mode

Indica o método aplicado para alterar os dados registrados no Catálogo de endereços.

Address Book Change Item

Indica que item no Catálogo de endereços foi alterado.

Address Book Change Request IP Address

Indica o tipo de endereço IP (IPv4/IPv6) do usuário utilizando o Catálogo de endereços.

Lockout/Release

Indica o status do bloqueio.

Valor	Conteúdo
Lockout	Ativação de bloqueio de senha
Release	Desativação de bloqueio de senha.

Lockout/Release Method

Indica o método aplicado para liberar o bloqueio.

Valor	Conteúdo
Manual	O equipamento foi bloqueado manualmente.
Auto	O equipamento foi desbloqueado pelo timer de liberação de bloqueio.

Lockout Release Target Administrator

Indica qual(is) administrador(es) é(são) liberado(s) após o desbloqueio.

Counter to Clear

Indica que contador é redefinido para cada usuário.

Export Target

Indica as definições a serem incluídas no arquivo de definição do dispositivo a ser exportado.

Valor	Conteúdo
System Settings	Definições do sistema
Copier Features	Recursos da copiadora

Valor	Conteúdo
Printer Features	Funções da impressora
Scanner Features	Recursos do scanner
Program (Copier)	Programa (Copiadora)
Program (Scanner)	Programa (Scanner)
Program (Document Server)	Programa (Servidor de documentos)
Web Image Monitor Setting	Definição do Web Image Monitor
Web Service Settings	Definições de serviços da Web
System/Copier SP	Sistema/Copiadora SP
Scanner SP	Scanner SP
Printer SP	Impressora SP

Target File Name

Indica o nome do arquivo de informações do dispositivo a ser importado ou exportado.

Stored File ID

Identifica um arquivo criado ou excluído.

Esta é uma ID hexadecimal que indica arquivos armazenados criados ou excluídos.

Stored File Name

Indica o nome de um arquivo criado ou excluído.

Delete File Type

Indica o tipo de exclusão de arquivo.

Valor	Conteúdo
Delete Normal File	Exclusão de arquivo normal
Delete Editing File	Exclusão durante a edição
Auto Delete	Exclusão de arquivo automática
Others	Exclusão de arquivo por outro motivo

Folder Number

Indica o número da pasta.

Folder Name

Indica o nome da pasta.

Creating/Deleting Folders

Indica as operações realizadas em pastas.

Valor	Conteúdo
Delete Folder	Pasta excluída
New Folder	Pasta criada

File Location

Indica a origem de todos os arquivos excluídos. "Document Server" indica a exclusão de todos os arquivos do disco rígido do equipamento.

Collect Job Logs

Indica o status da definição da coleta de logs de trabalhos.

Valor	Conteúdo
Active	A definição da coleta de logs de trabalhos é ativada.
Inactive	A definição de coleta de logs de trabalho é desativada.
Not Changed	Não foram efetuadas alterações na definição da coleta de logs de trabalhos.

Collect Access Logs

Indica o status da definição de coleta de logs de acessos.

Valor	Conteúdo
Active	A definição de coleta de logs de acessos é ativada.
Inactive	A definição de coleta de logs de acessos é desativada.
Not Changed	Não foram efetuadas alterações na definição de coleta de logs de acesso.

Collect Eco-friendly Logs

Indica o status da definição da coleta de logs ecológicos.

Valor	Conteúdo
Active	A definição da coleta de logs ecológicos é ativada.
Inactive	A definição da coleta de logs ecológicos é desativada.
Not Changed	Não foram efetuadas alterações na definição da coleta de logs ecológicos.

Transfer Logs

Indica o status da definição de transferência de logs.

Valor	Conteúdo
Active	A definição de transferência de log é ativada.
Inactive	A definição de transferência de log é desativada.
Not Changed	Não foram efetuadas alterações na definição de transferência de log.

Log Type

Se uma definição de nível de coleta de logs foi alterada, essa função indica detalhes da alteração.

Valor	Conteúdo
Job Log	Log de trabalhos
Access Log	Log de acessos
Eco-friendly Log	Log ecológico

Log Collect Level

Indica o nível da coleta de logs.

Valor	Conteúdo
Level 1	Nível 1
Level 2	Nível 2
User Settings	Definições do usuário

Encryption/Cleartext

Indica se a criptografia de comunicação está ativada ou desativada.

Valor	Conteúdo
Encryption Communication	A criptografia é ativada.
Cleartext Communication	A criptografia é desativada.

Machine Port No.

Indica o número da porta do equipamento.

Protocol

Protocolo de destino.

"Unknown" indica que o protocolo de destino não pôde ser identificado.

IP Address

Endereço IP de destino.

Port No.

Número de porta de destino.

Número de portas indicado em decimal.

MAC Address

Endereço MAC (físico) de destino.

Primary Communication Protocol

Indica o protocolo de comunicação primário.

Secondary Communication Protocol

Indica o protocolo de comunicação secundário.

Encryption Protocol

Indica o protocolo utilizado para criptografar a comunicação.

Communication Direction

Indica a direção da comunicação.

Valor	Conteúdo
Communication Start Request Receiver (In)	O equipamento recebeu uma solicitação para iniciar a comunicação.
Communication Start Request Sender (Out)	O equipamento enviou uma solicitação para iniciar a comunicação.

Communication Start Log ID

Indica a ID de registo para a hora de início da comunicação.

Esta é uma ID hexadecimal que indica a hora a que a comunicação teve início.

Communication Start/End

Indica as horas a que a comunicação teve início e terminou.

Network Attack Status

Indica o status do equipamento quando ocorrem ataques à rede.

Valor	Conteúdo
Violation Detected	Foi detectado um ataque à rede.
Recovered from Violation	A rede se recuperou de um ataque.
Max. Host Capacity Reached	O equipamento ficou inoperante pois o volume de dados recebidos atingiu a capacidade de hospedagem máxima.
Recovered from Max. Host Capacity	O equipamento ficou novamente inoperante depois de uma redução do volume de dados recebidos.

Network Attack Type

Identifica tipos de ataque de rede.

Valor	Conteúdo
Password Entry Violation	Quebra de senha
Device Access Violation	Ataque de negação de serviço (DoS)
Request Falsification Violation	Solicitação forjada

Network Attack Type Details

Indica detalhes de tipos de ataque à rede.

Valor	Conteúdo
Authentication Error	Erro de autenticação
Encryption Error	Erro de criptografia

Network Attack Route

Identifica a rota de ataque à rede.

Valor	Conteúdo
Attack from Control Panel	Ataque de uma operação não autorizada utilizando o painel de controle do equipamento
Attack from Other than Control Panel	Ataque por meio diferente de uma operação não autorizada utilizando o painel de controle do equipamento

Login User Name used for Network Attack

Identifica o nome de usuário de login usado no ataque à rede.

Add/Update/Delete Firmware

Indica o método utilizado para adicionar, atualizar ou excluir o firmware do equipamento.

Valor	Conteúdo
Updated with SD Card	Um cartão SD foi utilizado para realizar a atualização de firmware.
Added with SD Card	Um cartão SD foi usado para instalar o firmware.
Deleted with SD Card	Um cartão SD foi utilizado para excluir o firmware.
Moved to Another SD Card	O firmware foi transferido para outro cartão SD.
Updated via Remote	O firmware foi atualizado a partir de um computador remoto.
Updated for Other Reasons	A atualização de firmware foi realizada utilizando um método diferente dos métodos acima.

Module Name

Nome do módulo de firmware.

Parts Number

Número da parte do módulo de firmware.

Version

Versão do firmware.

Machine Data Encryption Key Operation

Indica o tipo de operação de chave de criptografia realizada.

Valor	Conteúdo
Back Up Machine Data Encryption Key	Foi realizado um backup de chave de criptografia.
Restore Machine Data Encryption Key	Uma chave de criptografia foi recuperada.
Clear NVRAM	O NVRAM foi eliminado.
Start Updating Machine Data Encryption Key	Foi iniciada uma atualização de chave de criptografia.
Finish Updating Machine Data Encryption Key	Uma atualização de chave de criptografia foi concluída.

Machine Data Encryption Key Type

Identifica o tipo de chave de criptografia.

Valor	Conteúdo
Encryption Key for Hard Disk	Chave de criptografia para disco rígido
Encryption Key for NVRAM	Chave de criptografia para NVRAM
Device Certificate	Certificado do dispositivo

Validity Error File Name

Indica o nome do ficheiro onde foi detectado um erro de validade.

Configuration Category

Indica as categorias com definições alteradas.

Valor	Conteúdo
User Lockout Policy	Política de bloqueio de usuário
Auto Logout Timer	Timer de logout automático
Device Certificate	Certificado do dispositivo
IPsec	IPsec
Compulsory Security Stamp	Carimbo obrigatório de segurança
S/MIME	S/MIME

Valor	Conteúdo
WIM Auto Logout Timer	Web Image Monitor auto logout timer
Extended Security	Segurança estendida
Firmware Update Start	Actualização do firmware
Prohibit printing stored files from Web Image Monitor	Proibir impressão de arquivos armazenados no Web Image Monitor

Configuration Name / Configuration Value

Indica os atributos das categorias.

Indica os valores dos atributos.

Atributo	Descrição
Lockout	É registrado se o bloqueio está ativo (Active) ou inativo (Inactive).
Number of Attempts before Lockout	É registrado o número de vezes que um usuário pode introduzir uma senha de início de sessão.
Lockout Release Timer	É registrado se o temporizador de liberação do bloqueio está ativo (Active) ou inativo (Inactive).
Lock Out User for	É registrado o tempo até a liberação do bloqueio.
Auto Logout Timer	É registrado se um timer de logout automático estiver definido como (On) ou (Off).
Auto Logout Timer (seconds)	É registrado o tempo até a execução do encerramento automático da sessão.
Operation Mode	É registrado o tipo de operação.
Certificate No.	É registrado o número do certificado a ser usado.
Certificate No. : IEEE 802. 1X (WPA/WPA2)	É registrado o número do certificado para aplicações. Quando nenhum certificado é utilizado, é gravado "Do not Use".
Certificate No. : S/MIME	É registrado o número do certificado para aplicações. Quando um certificado não é utilizado, é gravado "Do not Use".

Atributo	Descrição
Certificate No. : IPsec	É registrado o número do certificado para aplicações. Quando nenhum certificado é utilizado, é gravado "Do not Use".
Certificate No. : Digital Signature PDF	É registrado o número do certificado para aplicações. Quando nenhum certificado é utilizado, é gravado "Do not Use".
Certificate No. : Digital Signature PDF/A	É registrado o número do certificado para aplicações. Quando nenhum certificado é utilizado, é gravado "Do not Use".
IPsec	É registrado se o IPsec está ativo (Active) ou inativo (Inactive).
Encryption Key Auto Exchange: Setting1-4: Remote Address	É registrado o endereço remoto.
Encryption Key Auto Exchange: Setting1-4, Default: Security Level	É registrado o nível de segurança. Quando [Somente autenticação] é selecionado, "Authentication Only" é registrado. Quando [Autenticação e criptografia de baixo nível] é selecionado, "Authentication and Low Level Encryption" é registrado. Quando [Autenticação e criptografia de alto nível] é selecionado, "Authentication and High Level Encryption" é registrado. Quando [Definições do usuário] é selecionado, "User Settings" é registrado.
Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	É registrado o método de autenticação usado para o formato de troca automática de chave. É registrado "PSK" ou "Certificate".
Compulsory Security Stamp	É registrado se [Carimbo de segurança obrigatório] está definido como (On) ou (Off).
Scanner: Email Sending	A assinatura é registrada quando o scanner é usado para enviar e-mail.

Atributo	Descrição
Document Server (Utility): Stored File Transferring	A assinatura é registrada quando o Servidor de documentos (utilitário) é usado para transmitir documentos nele armazenados.
WIM Auto Logout Timer (minutes)	O log do timer de logout automático do Web Image Monitor é registrado em incrementos de 1 minuto.
Update Firmware	A entrada de log que relata as alterações na definição [Update Firmware] (Firmware de atualização) foi gravada. "Prohibit" ou "Do not Prohibit" foi gravado.
Change Firmware Structure	A entrada de log que relata as alterações na definição [Change Firmware Structure] (Alterar estrutura do firmware) foi gravada. "Prohibit" ou "Do not Prohibit" foi gravado.
Firmware Update Start	A entrada de log que relata a atualização do firmware foi gravada.
Prohibit printing stored files from Web Image Monitor	A entrada de log que relata alterações na definição [Prohibit printing stored files from Web Image Monitor] (Proibir a impressão de arquivos armazenados no Web Image Monitor) foi gravada. "Prohibit" ou "Do not Prohibit" foi gravado.

Destination Server Name

Indica o nome do servidor de destino para o qual as informações de rastreamento não foram enviadas quando o tipo de log é "Enhanced Print Volume Use Limitation: Tracking Permission Result".

Indica o nome do servidor do qual a solicitação de exportação ou importação de dados foi emitida quando o tipo de log for de importação ou exportação de informações de preferência.

HDD Format Partition

Indica a razão da formatação do disco rígido.

Valor	Conteúdo
HDD Exchange	O disco rígido foi substituído.
Problem with HDD Encryption Key	Há um problema com a chave de criptografia do disco rígido.

Valor	Conteúdo
Problem with Disk Label	O rótulo do disco não pode ser lido.
Problem with File System	Há um problema com o sistema de arquivos.

Access Result

Indica os resultados de operações registradas.

Valor	Conteúdo
Completed	Uma operação foi concluída com sucesso.
Failed	Uma operação foi concluída sem êxito.

Log de trabalho (origem)

Source

Indica a origem do arquivo de trabalho.

Valor	Conteúdo
Scan File	O arquivo de trabalho foi digitalizado.
Stored File	O arquivo de trabalho foi armazenado no disco rígido.
Printer	O arquivo de trabalho foi enviado ao driver da impressora.
Report	O arquivo de trabalho era um relatório impresso.

Start Date/Time

Indica quando as operações "Scan File", "Received File" e "Printer" foram iniciadas.

End Date/Time

Indica quando as operações "Scan File", "Received File" e "Printer" terminaram.

Stored File ID

Indica a ID dos dados produzidos como ficheiro guardado.

Esta é uma ID decimal que identifica o ficheiro guardado.

Stored File Name

Nomes de ficheiros "Stored File".

Folder Number

Indica o número da pasta em que o arquivo foi armazenado.

Folder Name

Indica o nome da pasta em que o arquivo foi armazenado.

Print File Name

Nome de ficheiros "Printer".

Log de trabalhos (destino)

Target

Tipo de destino do trabalho.

Valor	Conteúdo
Print	Print
Store	Armazenar
Send	Enviar

Start Date/Time

Indica quando as operações "Print", "Store" e "Send" iniciaram.

End Date/Time

Indica quando as operações "Print", "Store" e "Send" terminaram.

Destination Name

Nomes de destinos "Send".

Destination Address

Endereço IP, caminho ou endereço de e-mail dos destinos "Send".

Stored File ID

Indica a ID dos dados produzidos como um ficheiro guardado.

Esta é uma ID decimal que identifica o ficheiro guardado.

Stored File Name

Indica o nome do arquivo armazenado quando o Tipo de destino for "Store".

Folder Number

Indica o número da pasta em que você armazenou o arquivo.

Folder Name

Indica o nome da pasta em que você armazenou o arquivo.

Itens de informação de log ecológico

Start Date/Time

São registradas a data e a hora de início do evento.

End Date/Time

São registradas a data e a hora de término do evento.

Log Type

É registrado o tipo de registro ecológico.

Valor	Conteúdo
Main Power On	Ligado
Main Power Off	Desligado
Power Status Transition Result	Resultado de transição do status de energia
Job Related Information	Informações relacionadas ao trabalho
Paper Usage	Uso de papel
Power Consumption	Consumo de energia

Log Result

É mostrado se o evento terminou ou não.

Valor	Conteúdo
Completed	Concluído
Failed	Falha

Result

É registrado o resultado do evento.

Valor	Conteúdo
Succeeded	Êxito
Failed	Falha

Log ID

Identifica a ID atribuída ao log. Essa é uma ID hexadecimal que identifica o log.

Power Mode

É registrado o estado de energia do equipamento (após a transição de estado).

Valor	Conteúdo
Standby	Modo de espera
Low Power	Status de baixa energia
Silent	Status silencioso
HDD On	Status de HD ligado
Engine Off	Status de motor desligado
Controller Off	Status de controlador desligado
STR	Status de STR
Silent Print	Status de impressão silenciosa
Low Power Print	Status de impressão de baixa energia
Fusing Unit Off	Status de unidade de fusão desligada

Log Type

É registrado o tipo de registro de trabalho.

Job Interval (seconds)

Indica o tempo decorrido do início do trabalho anterior até o início do trabalho atual.

Job Duration (seconds)

Indica o tempo decorrido do início ao fim do trabalho.

Paper Usage (Large Size)

Indica o número de impressões em um lado por hora em papel grande.

Tamanho grande significa A3 (11 × 17 polegadas) ou maior.

Paper Usage (Small Size)

Indica o número de impressões em um lado só hora em papel pequeno.

Tamanho pequeno significa A3 (11 × 17 polegadas) ou menor.

Paper Usage (2 Sided: Large Size)

Indica o número de impressões duplex por hora em papel grande.

Tamanho grande significa A3 (11 × 17 polegadas) ou maior.

Paper Usage (2 Sided: Small Size)

Indica o número de impressões duplex por hora em papel pequeno.

Tamanho pequeno significa A3 (11 × 17 polegadas) ou menor.

Detected Power

O status do consumo de energia do equipamento é medido e registrado no log enquanto o equipamento estiver sendo utilizado.

Valor	Conteúdo
Controller Standby	Modo de espera do controlador
STR	Modo suspender para RAM (STR)
Main Power Off	A alimentação principal está desligada.
Scanning/Printing	Digitalização e impressão simultâneas
Printing	Status de impressão do equipamento
Scanning	Status de digitalização do equipamento
Engine Standby	Status de espera do motor
Engine Low	Status de baixa energia do motor
Engine Night	Estado de silêncio do motor
Engine Total	Consumo de eletricidade total do equipamento
Fusing Unit Off	Status de unidade de fusão desligada

Power Consumption(Wh)

Indica o consumo de energia em cada estado de energia.

Especificar as definições de coleta de logs

Ative as definições de coleta para cada tipo de log e configure o nível de coleta.

Nível de coleta de logs

Se "Nível de coleta de log de trabalhos" estiver definido como [Nível 1], todos os logs de trabalho serão coletados.

Nível de coleta de log de acessos

Se "Nível de coleta de log de acessos" estiver definido como [Nível 1], os seguintes itens são gravados no log de acessos:

- Formato HDD
- Exclusão de todos os logs
- Alteração de definição de log
- Alteração de item de coleta de log

Se "Nível de coleta de log de acessos" estiver definido como [Nível 2], todos os logs de acesso serão coletados.

Nível de coleta de logs ecológicos

Se "Nível de coleta de logs ecológicos" estiver definido como [Nível 1], os logs ecológicos não serão coletados.

Se "Nível de coleta de logs ecológicos" estiver definido como [Nível 2], todos os logs ecológicos serão coletados.

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Logs] em "Definições do dispositivo".**
4. **Selecione [Ativo] para cada função: "Coletar logs de trabalhos", "Coletar logs de acesso" e "Coletar logs ecológicos".**
5. **Especificar o nível de coleta para cada função, "Nível de coleta de log de trabalhos", "Nível de coleta de log de acesso", e "Nível de coleta de log ecológico".**

   Quando um nível é alterado, o status da seleção de detalhes do log muda de acordo com o nível.

   Para alterar itens individuais dos detalhes do log, faça uma configuração para cada item. Mesmo se o nível de coleta estiver definido como [Nível 1] ou [Nível 2], depois que cada item dos detalhes do log tiver sido alterado, o nível é alterado para [Definições de usuário].
6. **Clique em [OK].**
7. **É apresentada a mensagem "Atualizando...". Aguarde 1 ou 2 minutos e, em seguida, clique em [OK].**

   Se a tela anterior não aparecer novamente depois que você clicar em [OK], aguarde um pouco e clique no botão Atualizar do navegador da Web.
8. **Faça logout.**

- Quanto maior o valor do parâmetro "Nível de coleta de log de acessos", mais logs serão coletados.

Baixar logs

Utilize o seguinte procedimento para converter os logs armazenados no equipamento em um arquivo CSV para download em massa simultâneo.

Para coletar logs, configure a coleta do log de trabalhos, log de acesso e log ecológico como [Ativo]. Esta definição pode ser especificada em [Logs] na opção [Configuração] no Web Image Monitor.

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique na opção [Fazer download de logs] em "Definições do dispositivo".**
4. **Na caixa suspensa "Logs para download", selecione o tipo de log para baixar.**

   O log de segurança inclui 2 tipos de logs: logs de trabalhos e logs de acessos.
5. **Clique em [Download].**
6. **Especifique a pasta na qual você deseja salvar o arquivo.**
7. **Clique em [Voltar].**
8. **Faça logout.**

- Os logs baixados contêm os dados gravados até ao momento em que você clicar no botão [Download]. Os logs gravados depois que você clicar no botão [Download] não serão baixados. O campo "Result" da entrada de log para trabalhos não concluídos ficará em branco.
- O tempo de download varia de acordo como o número de logs.
- Se ocorrer um erro durante o download ou a criação do arquivo CSV, o download é cancelado e os detalhes do erro são incluídos no final do arquivo.
- Se um log for baixado com sucesso, aparecerá "Download completed." na última linha do arquivo de log.
- Para mais informações sobre como salvar arquivos de log CSV, consulte a Ajuda do seu navegador.
- Os arquivos de log baixados usam codificação de caracteres UTF-8. Para visualizar um arquivo de log, abra-o utilizando uma aplicativo que suporte UTF-8.
- Para detalhes sobre os itens contidos nos logs, consulte Pág. 200 "Atributos de logs que você pode baixar".

Número de logs que podem ser mantidos no equipamento

Quando o limite de logs de trabalhos, logs de acessos ou logs ecológicos que podem ser mantidos no equipamento é excedido e novos logs são gerados, os logs antigos são substituídos por novos. Se os logs não forem baixados periodicamente, talvez não seja possível gravar os logs antigos em arquivos.

Quando utilizar o Web Image Monitor para gerenciar logs, baixe os logs em um intervalo apropriado às condições indicadas na tabela.

Após baixar os logs, execute uma exclusão em massa dos logs.

Se você alterar a definição [Coletar]/[Não coletar] para a coleta de logs, você deve executar uma exclusão em massa dos logs.

Número máximo de logs que podem ser armazenados no equipamento

Tipos de log	Número máximo de logs
Logs de trabalhos	4000
Logs de acessos	12000
Logs ecológicos	4000

Números estimados de logs criados por dia

Tipos de log	Número de logs criados por dia
Logs de trabalhos	100
Logs de acessos	300 Esse número é baseado em 100 operações, como operações de inicialização e de acesso na Web, e 200 entradas de trabalhos (2 entradas por trabalho: 1 de login e 1 de logout).
Logs ecológicos	100

Nestas condições, o equipamento podem manter registros de 40 dias sem substituição. Recomendamos baixar logs a cada 20 dias caso ocorra algum erro.

O administrador do equipamento deve gerenciar adequadamente os arquivos de log baixados.

- Quando os logs estiverem sendo baixados, não execute nenhuma operação que crie entradas de log porque os logs sendo baixados não podem ser registrados como novas entradas.
- A exclusão em massa de logs pode ser executada no painel de controle ou por meio do Web Image Monitor.

Notas sobre a operação quando o número de entradas de logs atinge o máximo

Se o número de logs que podem ser armazenados no equipamento exceder o limite especificado, os logs antigos são substituídos por logs novos. O número máximo de logs que podem ser armazenados é definido para cada um dos logs de trabalhos, logs de acessos e logs ecológicos.

O log de trabalho e log de acesso são baixados como um arquivo único.

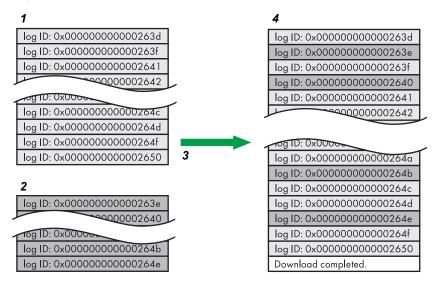
"Se os logs são baixados sem substituir" abaixo indica que o log de trabalho e o log de acesso são combinados após o download.

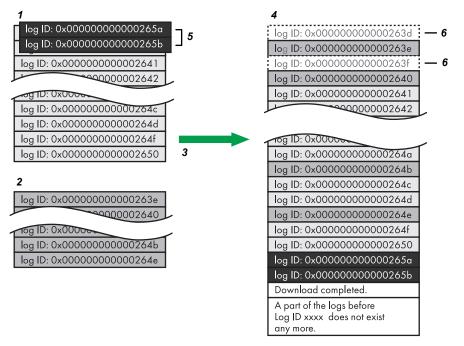
"Se os logs são baixados durante a substituição" abaixo indica que parte do log de acesso será substituído.

Nesse exemplo, parte do log de acesso foi substituído por um log baixado e excluído.

O log ecológico é baixado como um arquivo independente.

As entradas de log são substituídas na ordem de prioridade. As entradas do log com prioridade mais alta não serão substituídas ou excluídas.

Se os logs forem baixados sem substituição

1. **Log de acessos**
2. **Log de trabalhos**
3. **Download**
4. **Logs baixados**

Se os logs forem baixados durante a substituição

1. **Log de acessos**
2. **Log de trabalhos**
3. **Download**
4. **Logs baixados**
5. **Substituição**
6. **Excluídos por substituição**

Verifique a mensagem na última linha dos logs baixados para determinar se a substituição ocorreu ou não durante o download dos logs.

- Se a substituição não ocorreu, a última linha apresentará a seguinte mensagem: Download completed.
- Em caso de sobregravação, a última linha conterá a seguinte mensagem: Download completed. A part of the logs before Log ID xxxx does not exist any more.

- Se ocorrer substituição, parte dos logs será excluída pela substituição, portanto, verifique o log "Log ID xxxx" e os logs mais recentes.

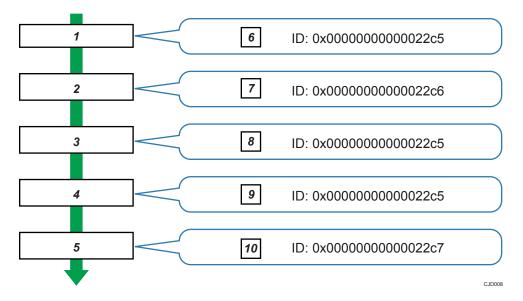
Logs de trabalhos de impressão

As entradas de log de impressão registradas antes de a entrada de login registrada no log de acessos.

Detalhes dos trabalhos (recepção, processamento, saída dos dados dos trabalhos, e etc.) são registradas como entradas únicas.

Quando o equipamento recebe um trabalho de impressão, ele cria uma ID para o trabalho e a registra no log de trabalhos. O equipamento cria então uma ID de login para o trabalho de impressão e a registra no log de acessos. Depois disso, cria uma entrada de log de trabalho com detalhes do trabalho que é processado e saída (com a mesma ID de login). Quando o equipamento conclui o processamento do trabalho, ele cria uma entrada de logout e a registra no log de acessos.

As entradas com detalhes sobre operações como recebimento, processamento e saída de uma série de trabalhos de impressão são criadas primeiro no log de trabalhos e, em seguida, os detalhes do login e logout são registrados no log de acessos.

Fluxograma do trabalho de impressão

1. **Os dados do trabalho de impressão são recebidos.**
2. **Os dados de autenticação (login) são recebidos.**
3. **O trabalho de impressão é processado.**
4. **O trabalho de impressão é concluído.**
5. **Os dados de autenticação (login) são recebidos.**
6. **Uma ID é atribuída ao trabalho de impressão e registrada como uma entrada no log de trabalhos.**
7. **Os dados de autenticação (login) são registrados como uma entrada no log de acessos.**

8. **As informações sobre o processamento do trabalho de impressão são registradas como uma entrada no log de trabalhos (usando a mesma ID).**
9. **As informações sobre a saída do trabalho de impressão são registradas como uma entrada no log de trabalhos (usando a mesma ID).**
10. **Os dados de autenticação (logout) são registrados como uma entrada no log de acessos.**

Excluir todos os logs

Utilize o seguinte procedimento para excluir todos os logs armazenados no equipamento.

"Excluir todos os logs" aparece se um dos logs de trabalho, logs de acesso ou logs ecológicos estiver definido como [Ativo].

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Logs] em "Definições do dispositivo".**
4. **Clique em [Excluir] em "Excluir todos os logs".**
5. **Clique em [OK].**
6. **Faça logout.**

Desativar a transferência de logs para o Servidor de coleta de logs

Use o seguinte procedimento para desativar a transferência de logs para o servidor de coleta de logs. Observe que você só pode alternar a definição de transferência de logs para [Inativo] se [Ativo] já estiver definido.

1. **Faça login como administrador do equipamento no Web Image Monitor.**
2. **Aponte para [Gerenciamento do dispositivo] e clique em [Configuração].**
3. **Clique em [Logs] em "Definições do dispositivo".**
4. **Selecione [Inativo] na área [Transferir logs] em "Definições comuns para todos os logs".**
5. **Clique em [OK].**
6. **Faça logout.**

Gerenciar logs do equipamento

Você pode especificar definições, como coleta de logs, se deseja ou não transferir logs para o servidor de coleta de logs e excluir ou não todos os logs.

Especificar as definições de coleta de logs

Habilitar as definições de coleta para cada tipo de log.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 4 vezes.**
5. **Pressione [Coletar logs].**
6. **Selecione [Ativo] para cada função: "Log de trabalhos", "Log de acessos" e "Logs ecológicos".**
7. **Pressione [OK].**
8. **Faça logout.**
9. **Desligue o equipamento e, em seguida, religue-o novamente.**

Desativar a transferência de logs para o Servidor de coleta de logs

Execute o procedimento a seguir para desativar a transferência de logs do equipamento para o servidor de coleta de logs. Observe que você só pode alternar a definição da transferência de logs para [Desligado] se essa definição estiver definida como [Ligado].

Para mais informações sobre o servidor de coleta de logs, consulte o seu representante comercial.

Para mais detalhes sobre a definição do log de transferência, consulte o manual do servidor de coleta de logs.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**
5. **Pressione [Definição do log de transferência].**
6. **Pressione [Desligado].**
7. **Pressione [OK].**
8. **Faça logout.**

Especificar Excluir todos os logs

Utilize o seguinte procedimento para excluir todos os logs armazenados no equipamento.

A exclusão de todos os logs do equipamento em lote pode ser executada apenas se o servidor de coleta de logs estiver sendo usado ou se a definição Web Image Monitor tiver sido especificada para coletar logs de trabalhos, logs de acesso ou logs ecológicos.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**
5. **Pressione [Excluir todos os logs].**
6. **Pressione [Sim].**
7. **Pressione [Sair].**
8. **Faça logout.**

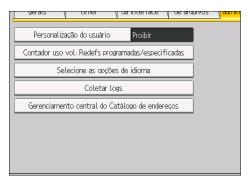
Gerenciar logs a partir do Servidor de coleta de logs

Para mais informações sobre o uso do servidor de coleta de logs para gerenciar arquivos de logs, consulte o manual fornecido com o servidor de coleta de logs.

Configurar a tela principal para usuários individuais

Permite que cada usuário use sua própria tela principal.

Quando um usuário faz o login, a tela principal personalizada é exibida.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 4 vezes.**
5. **Pressione [Personalização do usuário].**

6. **Pressione [Permitir] e, em seguida, [OK].**
7. **Faça logout.**

- Essa opção pode ser configurada também usando o Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- As informações da tela inicial de cada usuário são mantidas mesmo quando a "Personalização do usuário" está definida para [Proibir]. Quando a definição é restaurada para [Permitir], as informações podem ser utilizadas novamente.

Avisos sobre o uso de telas iniciais do usuário

Observe os seguintes avisos antes de utilizar esta função.

- Quando um usuário é registrado no livro de endereços, é criada uma tela principal para esse usuário. A tela principal do usuário é configurada com as definições predefinidas (organização de ícones).

- Se a opção Proteção de menus estiver definida em [Nível 1] ou [Nível 2], o usuário não pode usar as funções de registro, edição ou exclusão da tela. No entanto, o usuário pode adicionar ícones à sua tela principal.
- Depois que Menu Protect (Proteção de menus) for definido como [Level 1] (Nível 1) ou [Level 2] (Nível 2), peça ao administrador do equipamento que crie os programas necessários.
- Somente os ícones das funções que o usuário tem permissão para usar são exibidos.
- Quando um usuário é excluído do Catálogo de endereços, as informações da tela principal do usuário também são excluídas.
- Quando um usuário edita um programa, as alterações são indicadas nas telas principais dos usuários que tenham o ícone do programa nas suas telas principais.
- Quando um usuário exclui um programa, o ícone do programa é excluído das telas principais de todos os usuários que tenham o ícone do programa nas suas telas principais.
- Com o fato de cada usuário poder personalizar sua tela principal, o administrador não pode verificar as informações da tela principal de cada usuário.

Gerenciar informações de dispositivos

⚠CUIDADO

- Mantenha cartões SD ou dispositivos USB de memória flash fora do alcance de crianças. Se uma criança engolir acidentalmente um cartão SD ou um dispositivo USB de memória flash, procure um médico imediatamente.

As informações do dispositivo do equipamento podem ser configuradas por um administrador com privilégios para gerenciar dispositivos, usuários, redes e arquivos.

As informações de dispositivo do equipamento podem ser exportadas para um dispositivo externo como um arquivo de informações de definição do dispositivo. Ao importar um arquivo de informações de definição de dispositivo exportado para o equipamento, ele poderá ser usado como arquivo de backup para restaurar as definições do dispositivo.

Além disso, o gerenciamento do arquivo de informações de definições com o servidor de gerenciamento de dispositivo permite que o arquivo de informações de definições do dispositivo seja importado periodicamente em um horário especificado ou na inicialização do dispositivo.

Dados que podem ser importados e exportados

- Recursos do servidor de copiadora/documentos
- Características da impressora
- Recursos de scanner
- Programa (Serv docs)
- Programa (Copiadora)
- Programa (Scanner)
- Def monitor imag da Web
- Configurações de serviço da Web
- Configurações do sistema

Dados que não podem ser importados ou exportados

- Algumas definições do sistema*1 *2

*1 A definição da data, definições que requerem certificados de dispositivos e definições que precisam ser ajustadas para cada máquina (por exemplo, definições de ajuste de imagem) não podem ser importadas ou exportadas.

*2 Definições para apenas executar funções e definições para exibição somente não podem ser importadas ou exportadas.

- Definições de recurso estendido
- Catálogo de endereços
- Programas (função de impressora)
- Carimbo do usuário em Recursos do servidor de copiadora/documentos

- Definições que podem ser especificadas via telnet
    - Dados relacionados ao @Remote
    - Contadores
    - Definições da unidade de impressora externa
    - Definições que podem ser especificadas apenas via Web Image Monitor ou serviço da Web (por exemplo, definição Bonjour, SSDP)

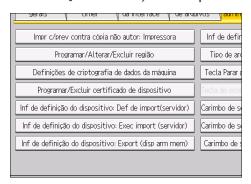
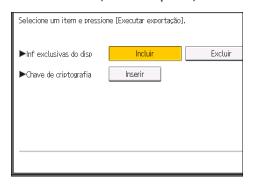
- O formato de arquivo para exportações é CSV.
- A configuração de dispositivo do equipamento que está importando o arquivo de informações de definição de dispositivo deve ser igual à configuração do equipamento que exportou o arquivo de informações de definição de dispositivo. Caso contrário, o arquivo de informações de definição de dispositivo não poderá ser importado.
- A importação e exportação entre equipamentos só é possível se os modelos, região de uso e as configurações dos dispositivos abaixo coincidirem.
    - Bandeja de entrada
    - Bandeja de saída
    - Equipado ou não com finalizador e tipo de finalizador
    - ADF
- Se a configuração de dispositivo for alterada, exporte o arquivo de informações de definição de dispositivo atualizado.
- Se houver equipamentos com a mesma configuração de dispositivo, é possível especificar suas definições de maneira idêntica, importando o mesmo arquivo de definição de dispositivo.
- Se a tela inicial contiver arquivos de imagem JPG, eles também serão exportados.
- Enquanto um usuário utiliza o equipamento, nada pode ser importado ou exportado até que o usuário termine a operação do equipamento.
- Durante operações de exportação e importação, o equipamento não pode ser utilizado de nenhuma outra maneira.
- Para obter mais detalhes sobre o manuseamento de cartões SD, consulte Getting Started.
- Também é possível usar o Web Image Monitor para configurar as definições de importação, exportação e servidor.

Exportar informações de dispositivo

Quando as informações do dispositivo são exportadas através do painel de controle, os dados são salvos em um cartão SD.

1. **Introduza um cartão SD no slot apropriado na parte lateral do painel de controle.**

   Para obter informações sobre como inserir o cartão SD, consulte Getting Started.

2. **Faça login pelo painel de controle como administrador com os privilégios de administrador de usuários, administrador do equipamento, administrador de rede e administrador de arquivos.**
3. **Pressione [Definições do sistema].**
4. **Pressione [Ferramentas admin].**
5. **Pressione [▼Próximo] 3 vezes.**
6. **Pressione [Inf de definição do dispositivo: Import (disp arm mem)].**

7. **Defina as condições de exportação.**

   - Especifique a opção [Incluir] ou [Excluir] as "Inf exclusivas do disp". "Inf exclusivas do disp" incluem o endereço IP, nome do host, etc.
   - Especifique uma chave de criptografia.

8. **Pressione [Executar exportação].**
9. **Pressione [OK].**
10. **Pressione [Sair].**
11. **Faça logout.**

7

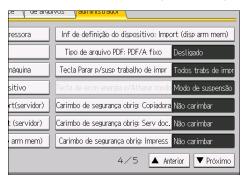
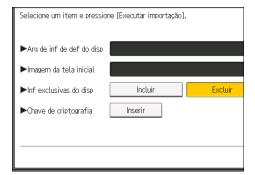
- Se a importação ou exportação falhar, você pode procurar o erro no log. O log é armazenado no mesmo local do arquivo de informações de definições do dispositivo.

Importar informações de dispositivo

Importar informações de dispositivo salvas em um cartão SD.

1. **Introduza um cartão SD no slot apropriado na parte lateral do painel de controle.**

   Para obter informações sobre como inserir o cartão SD, consulte Getting Started.

2. **Faça login pelo painel de controle como administrador com os privilégios de administrador de usuários, administrador do equipamento, administrador de rede e administrador de arquivos.**
3. **Pressione [Definições do sistema].**
4. **Pressione [Ferramentas admin].**
5. **Pressione [▼Próximo] 3 vezes.**
6. **Pressione [Inf definição dispositivo:Import (disp arm mem)].**

7. **Configure as condições de importação.**

- Pressione [Selecionar] no "Arq de inf de def do disp" para selecionar o(s) arquivo(s) para importar.

- Ao adicionar uma imagem à tela inicial, pressione [Selecionar] para "Imagem da tela inicial" e, em seguida, selecione o arquivo.
- Especifique a opção [Incluir] ou [Excluir] as "Inf exclusivas do disp". "Inf exclusivas do disp" incluem o endereço IP, nome do host, etc.
- Insira a chave de criptografia especificada quando o arquivo foi exportado.

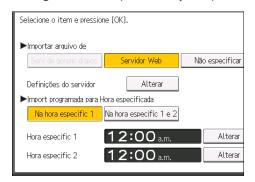
8. **Pressione [Executar importação].**
9. **Pressione [OK].**
10. **Pressione [Sair].**

    O equipamento é reiniciado.

- Se a importação ou exportação falhar, você pode procurar o erro no log. O log é armazenado no mesmo local do arquivo de informações de definições do dispositivo.

Importar informações de dispositivo periodicamente

Essa definição importa automaticamente as informações do dispositivo armazenadas em um servidor para o equipamento.

1. **Faça login pelo painel de controle como administrador com os privilégios de administrador de usuários, administrador do equipamento, administrador de rede e administrador de arquivos.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Inf de definição do dispositivo: Def de import(servidor)].**
6. **Configure as condições de importação.**

- Selecione a origem dos arquivos de importação. Configure as definições como URL, nome de usuário, senha, etc., usando as definições dessas informações no servidor.

- Selecione a frequência de importação dos arquivos de informações do dispositivo e defina a hora específica para a importação periódica.
- Selecione se um arquivo de informações de configuração do dispositivo deverá ser importado ou não caso seja idêntico ao último arquivo importado.
- Se o arquivo de informações de configuração do dispositivo a ser importado estiver criptografado, defina uma chave de criptografia.
- Selecione se o administrador do equipamento deve receber ou não uma notificação de e--mail em caso de falha da importação.

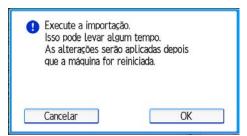
7. **Pressione [OK].**
8. **Faça logout.**

- Essa opção pode ser configurada também usando o Web Image Monitor. Para mais informações, consulte a Ajuda do Web Image Monitor.
- Mais definições detalhadas de importação poderão ser feitas se o servidor de gerenciamento de dispositivo for utilizado. Para obter mais detalhes, consulte o manual do usuário do servidor de gerenciamento de dispositivo.
- Se a importação ou exportação falhar, você pode procurar o erro no log. O log é armazenado no mesmo local do arquivo de informações de definições do dispositivo.

Importar manualmente o arquivo de informações de configuração do dispositivo a partir de um servidor

Importe manualmente para o equipamento o arquivo de informações de definições do dispositivo especificado com [Inf de definição do dispositivo: Def de import(servidor)].

1. **Faça login pelo painel de controle como administrador com os privilégios de administrador de usuários, administrador do equipamento, administrador de rede e administrador de arquivos.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] 3 vezes.**
5. **Pressione [Inf de definição do dispositivo: Exec import (servidor)].**

6. **Pressione [OK].**

7. **Pressione [Sair].**

   O equipamento é reiniciado.

- Se a importação ou exportação falhar, você pode procurar o erro no log. O log é armazenado no mesmo local do arquivo de informações de definições do dispositivo.

Solução de problemas

Se ocorrer um erro, verifique primeiro o código do resultado do log. Valores diferentes de 0 indicam que ocorreu um erro. O código do resultado aparecerá na área circulada ilustrada a seguir.

Exemplo de um arquivo de log

```
"1.0.0"
"ExecType", "Date", "SerialNo",PnP", "Model", "Destination","IP","Host","Storage","FileNam
e","FileID","TotalItem","NumOfOkItem","ResultCode","ResultName","Identifier"
"IMPORT"
"20XX-07-05T15:29:16+09:00"
"3C35-7M0014"
"Brand Name"
"Product Name"
"0"
"10"
"10.250.155.125"
"RNP00267332582D"
"SD"
"20XX07051519563C35-710220.csv"
"20XX07051519563C35-710220"
"    0"
" 2"
REQUEST"
"TargetID","ModuleID","PrefID","Item","NgCode","NgName"
```

CJD023

Se não conseguir resolver o problema ou não souber como resolvê-lo depois de verificar o código, anote a entrada do log de erro e entre em contato com a assistência técnica.

ResultCode	Causa	Soluções
2 (INVALID REQUEST)	Houve uma tentativa de importar um arquivo entre diferentes modelos ou equipamentos com diferentes configurações de dispositivos.	Importe arquivos exportados do mesmo modelo com as mesmas configurações do dispositivo.
4 (INVALID OUTPUT DIR)	Falha ao gravar as informações do dispositivo no dispositivo de destino.	Verifique se o dispositivo de destino está operando normalmente.
7(MODULE ERROR)	Ocorreu um erro inesperado durante uma importação ou exportação.	Desligue e ligue a energia e tente a operação novamente. Se o erro persistir, entre em contato com a assistência técnica.
8 (DISK FULL)	O espaço de armazenamento disponível na mídia externa é insuficiente.	Execute a operação novamente depois de se certificar de que existe espaço de armazenamento suficiente.
9 (DEVICE ERROR)	Falha ao gravar ou ler o arquivo de log.	Verifique se o caminho para a pasta para armazenar o arquivo ou a pasta na qual o arquivo está armazenado está indisponível.
10 (LOG ERROR)	Falha ao gravar o arquivo de log. O disco rígido está defeituoso.	Contate a assistência técnica.

ResultCode	Causa	Soluções
20 (PART FAILED)	Falha ao importar algumas definições.	O motivo para a falha está registrado em "NgName". Verifique o código. **Motivo do erro (NgName)** 2 INVALID VALUE O valor especificado excede ao intervalo permitido. 3 PERMISSION ERROR A permissão para editar a definição está indisponível. 4 NOT EXIST A definição não existe no sistema. 5 INTERLOCK ERROR A definição não pode ser alterada devido ao status do sistema ou por estar associada a outras definições específicas. 6 OTHER ERROR A definição não pode ser alterada por algum outro motivo.
21 (INVALID FILE)	Falha ao importar o arquivo porque ele está no formato errado na mídia externa.	Verifique se o formato do arquivo está correto. O log está no formato de arquivo CSV.
22 (INVALID KEY)	A chave de criptografia não é válida.	Use a chave de criptografia correta.

Gerenciar o contador ecológico

As informações do contador ecológico são exibidas no login quando a autenticação do usuário é utilizada.

O contador ecológico indica a frequência do uso de impressão a cores, duplex ou combinada no total de folhas impressas.

Além disso, o índice ecológico indica a economia com toner e papel. O índice ecológico mais alto resulta em maior economia de recursos.

- Quando a autenticação Básica, do Windows ou LDAP é utilizada para autenticação do usuário, o equipamento compila os dados e exibe um contador ecológico para cada usuário.
- Quando utilizada a autenticação de código de usuário para a autenticação do usuário ou quando a autenticação do usuário não está em uso, o equipamento compila os dados e exibe um contador ecológico geral.

Configuração dos contadores ecológicos

Defina o período de coleta de dados para o contador ecológico e uma mensagem do administrador.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Período do contador ecológico/Mensagem do administr].**
6. **Altere as definições.**
7. **Pressione [OK].**
8. **Pressione [Sair].**
9. **Faça logout.**

Período de contagem

Definição do período para coleta de dados para o contador ecológico.

Quando [Especificar dias] for selecionado, os dados para o contador ecológico serão compilados de acordo com o número de dias especificado.

Predefinição: [**Não contar**]

Mensagem do administrador

Selecione a mensagem a ser exibida quando um usuário faz login.

Uma mensagem padrão é exibida ao selecionar "Mensagem fixa 1" ou "Mensagem fixa 2".

Se você selecionar "Mensagem do usuário", o administrador do equipamento pode inserir uma mensagem para ser exibida.

Padrão: [Mensagem fixa 1]

Exibir tela de informações

Especifique se deseja exibir a tela de informações no login do usuário.

Padrão: [Desligado]

Tempo da tela

Especifica quando a tela de informações é exibida.

Predefinição: [Sempre que fizer login]

Redefinir o contador ecológico de um equipamento

O contador ecológico de um equipamento pode ser redefinido.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Exibir/Apagar contador ecológico].**
5. **Pressione [Limpar valor atual] ou [Limp valor atual e ant.].**
6. **Pressione [OK].**
7. **Faça logout.**

Redefinir contadores ecológicos de usuários

Ao redefinir o contador ecológico dos usuários, os contadores ecológicos de todos os usuários são redefinidos.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Exibir/Apagar contador ecológico por usuário].**
5. **Pressione [Limpar valor atual] ou [Limp valor atual e ant.].**
6. **Pressione [OK].**
7. **Faça logout.**

Gerenciar o Catálogo de endereços

Especificar a Exclusão automática de dados do Catálogo de endereços

Especifique como o equipamento processa uma solicitação de registro automático depois que os dados registrados no Catálogo de endereços tenham atingido o limite.

Se você definir [Ligado], novas contas de usuários serão adicionadas ao excluir automaticamente contas de usuários antigas.

As contas não utilizadas pelo maior período de tempo serão excluídas primeiro.

Se você definir como [Desligado], as contas de usuários antigas não são excluídas; portanto, novas contas de usuários não podem ser adicionadas quando o limite de dados registrados chegar ao máximo.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [Excluir aut usuário no Cat de end].**
5. **Selecione [Ligado] e, em seguida, [OK].**
6. **Faça logout.**

- Os dados são excluídos automaticamente somente quando o equipamento recebe uma solicitação para registrar os dados.

  A exclusão automática não será executada se as contas de usuários forem adicionadas manualmente.
- Somente as contas de usuário com códigos de usuário ou os nomes de usuários e senhas de login serão excluídos automaticamente.

Excluindo todos os dados do Catálogo de endereços

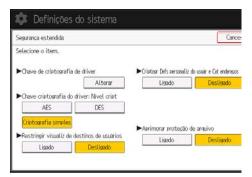
Você pode excluir todos os dados registrados no Catálogo de endereços.

1. **Faça login como administrador de usuário no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**

4. **Pressione [Excluir todos os dados no Catálogo de endereços].**
5. **Pressione [Sim] e, em seguida, [Sair].**
6. **Faça logout.**

Especificar as Funções de Segurança Avançadas

Além de proporcionar segurança básica através da autenticação do usuário e dos limites de acesso ao equipamento especificados pelo administrador, você pode aumentar a segurança criptografando os dados transmitidos e os dados no Catálogo de endereços.

1. **Inicie a sessão a partir do painel de controle como um administrador com privilégios.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo].**
5. **Pressione [Segurança estendida].**
6. **Pressione a definição que deseja alterar.**

7. **Pressione [OK].**
8. **Faça logout.**

- Os privilégios de operação de um administrador variam de acordo com as definições.

Código de encriptação do controlador

O administrador da rede pode especificar isto.

Especifique uma cadeia de texto para descriptografar senhas de login ou senhas de arquivos enviadas para o driver quando a autenticação de usuário está LIGADA.

Para especificar uma chave de criptografia de driver, registre a chave de criptografia especificada com o driver do equipamento.

Para mais informações, consulte Pág. 162 "Especificar uma chave de criptografia de driver".

Chave criptografia do driver: Nível cript

O administrador da rede pode especificar isto.

Especifique o grau de criptografia para enviar trabalhos do driver para o equipamento.

O equipamento verifica o grau de criptografia da senha anexada ao trabalho e o processa.

Quando a opção [Criptografia simples] é especificada, todos os trabalhos verificados pela autenticação de usuário são aceitos.

Quando a opção [DES] é especificada, os trabalhos criptografados com DES ou AES são aceitos.

Quando a opção [AES] é especificada, os trabalhos criptografados com AES são aceitos.

Se selecionar a opção [AES] ou a opção [DES], especifique a definição de criptografia usando o driver de impressão. Para mais informações sobre a especificação do driver de impressão, consulte a Ajuda do mesmo.

Predefinição: [**Criptografia simples**]

Restringir visualiz. informações utilizador

O administrador do equipamento pode especificar isto quando a autenticação de usuário está especificada.

Quando o histórico do trabalho é selecionado utilizando uma conexão de rede para a qual a autenticação não seja fornecida, todas as informações pessoais podem ser visualizadas como "********". Como as informações que identificam usuários registrados não podem ser exibidas, os usuários não autorizados são impedidos de obter informações sobre os arquivos registrados.

Padrão: [**Desligado**]

Criptogr Defs personaliz do usuár e Cat endereços

O administrador do usuário pode especificar isso.

Criptografar as definições individuais dos usuários do equipamento e os dados no Catálogo de endereços.

Mesmo que as informações internas do equipamento sejam obtidas ilegalmente, a criptografia impede que as definições de usuários individuais ou os dados do Catálogo de endereços sejam lidos.

Para mais informações, consulte Pág. 85 "Proteger o Catálogo de endereços".

Padrão: [**Desligado**]

Aprimorar proteção de arquivo

O administrador do arquivo pode especificar isso.

Ao especificar uma senha, o administrador de arquivos pode limitar operações como impressão, exclusão e envio de arquivos. Além disso, um administrador de arquivo pode evitar que usuários não autorizados acessem os arquivos. No entanto, ainda é possível evitar que as senhas sejam quebradas.

Ao especificar "Aprimorar proteção de arquivo", os arquivos são bloqueados e se tornam inacessíveis se uma senha inválida for digitada dez vezes. Isto pode proteger os arquivos de acesso de tentativas de acesso não autorizado com senhas aleatórias.

Se a função Aprimorar proteção de arquivo for habilitada, o ícone aparecerá na parte inferior direita da tela.

Os ficheiros bloqueados só podem ser desbloqueados pelo administrador de ficheiros.

Quando os arquivos estão bloqueados, não é possível selecioná-los mesmo quando a senha correta é inserida.

Padrão: [**Desligado**]

Restringir uso de destinos

O administrador do usuário pode especificar isso.

Os destinos de scanner disponíveis estão limitados aos destinos registrados no Catálogo de endereços.

Nenhum usuário pode inserir diretamente os destinos da transmissão.

Se você especificar a definição para receber e-mails via SMTP, não será possível usar "Restringir uso de destinos"

Os destinos buscados por "Busca LDAP" podem ser usados.

Para mais informações, consulte Pág. 65 "Restringir o uso de lista de destinos".

Padrão: [**Desligado**]

Restringir adição de destinos de usuários

O administrador do usuário pode especificar isso.

Se definir "Restringir adição de destinos de usuários", os usuários poderão registrar um destino de scanner no Catálogo de endereços simplesmente inserindo o destino e pressionando [Dest progr]. Caso essas funções sejam definidas como [Ligado], a tecla [Dest progr] não será exibida. Mesmo assim, os usuários podem inserir um destino diretamente, utilizando a tela do scanner, embora não possam registrar esse destino no Catálogo de endereços pressionando [Dest progr].

Além disso, mesmo que essas funções sejam definidas como [Ligado], os usuários registrados no Catálogo de endereços podem alterar suas senhas. Somente o administrador pode alterar itens diferentes da senha.

Padrão: [**Desligado**]

Definições em SNMPv1, v2

O administrador da rede pode especificar isto.

Se os protocolos SNMPv1 ou SNMPv2 são usados para acessar o equipamento, a autenticação não pode ser executada, por isso, as definições de papel ou outras definições especificadas pelo administrador do equipamento podem ser alteradas. Se seleccionar [Proibir], a definição pode ser visualizada mas não especificada com SNMPv1, v2.

Padrão: [**Não receber**]

Autenticar trabalho actual

O administrador do equipamento pode especificar isso.

Essa definição permite especificar se a autenticação é necessária ou não para operações como cancelamento de trabalhos nas funções de copiadora e impressora.

Se seleccionar [PrivilégioInícioSessão], podem utilizar o equipamento os utilizadores autorizados e o administrador do equipamento. Quando esta opção é seleccionada, não é necessária autenticação dos utilizadores que tenham iniciado sessão no equipamento antes de ter sido seleccionado o [PrivilégioInícioSessão].

Se especificar [Privilégio de acesso], qualquer usuário que tenha executado um trabalho de cópia ou impressão pode cancelar o mesmo. Além disso, o administrador da máquina pode cancelar o trabalho de cópia ou impressão do usuário.

Mesmo se tiver selecionado [Privilégio de início de sessão] e iniciou a sessão no equipamento, não poderá cancelar uma cópia ou um trabalho de impressão em curso se não tiver autorização para utilizar as funções de cópia e impressora.

Poderá especificar "Autenticar trabalho atual" somente se a opção "Gestão de autenticação de usuário" tiver sido especificada.

Padrão: [**Desligado**]

Política da palavra-passe

O administrador do usuário pode especificar isso.

Esta definição permite especificar [Definição de complexidade] e [N° mínimo de caracteres] para a senha. Com esta definição é possível usar somente as senhas que satisfaçam as condições especificadas em "Definição de complexidade" e "Nº mínimo de caracteres".

Ao selecionar [Nível 1], especifique uma senha usando 2 tipos de caracteres de letras maiúsculas, minúsculas, números decimais e símbolos como #.

Ao selecionar [Nível 2], especifique uma senha usando 3 tipos de caracteres de letras maiúsculas, minúsculas, números decimais e símbolos como #.

Padrão: [**Desligado**] Não há restrições quanto ao número de caracteres, e os tipos de caracteres não são especificados.

@Remote Service

O administrador do equipamento pode especificar isso.

A comunicação através de HTTPS para Serviço @Remote será desativada se você selecionar [Proibir].

Ao definir esta opção como [Proibir], consulte o representante de assistência técnica.

Se estiver definido como [Proibir alguns serv], será impossível alterar as definições via conexão remota, proporcionando uma operação segura.

Padrão: [**Não receber**]

Actualizar firmware

O administrador do equipamento pode especificar isso.

Esta definição é para especificar se atualizações de firmware devem ser permitidas ou não no equipamento. Um representante de serviço atualiza o firmware, ou o firmware é atualizado através da rede.

Se você selecionar [Proibir], o firmware do equipamento não pode ser atualizado.

Se seleccionar [Não proibir], não existem restrições nas actualizações de firmware.

Padrão: [Não receber]

Alterar estrutura do firmware

O administrador do equipamento pode especificar isso.

Esta definição é para especificar se é possível ou não evitar alterações na estrutura do firmware do equipamento. A função de Alterar Estrutura do Firmware detecta o status do equipamento quando o cartão SD é inserido, removido ou substituído.

Se você selecionar [Proibir], o equipamento para durante a inicialização se for detectada uma alteração da estrutura do firmware e aparece uma mensagem solicitando o login do administrador. Depois de o administrador do equipamento iniciar sessão, o equipamento termina a inicialização com o firmware atualizado.

O administrador pode verificar se a alteração da estrutura atualizada é permitida ou não verificando a versão do firmware visualizada na tela do painel de controle. Se a alteração da estrutura do firmware não for permitida, contacte o seu representante de assistência técnica antes de iniciar a sessão.

Se definir "Alterar estrutura de firmware" para [Proibir], a autenticação do administrador deve estar ativada.

Depois de especificar [Proibir], desative a autenticação de administrador. Quando a autenticação de administrador for ativada novamente, você poderá retornar a definição para [Não proibir].

Se seleccionar [Não proibir], a alteração da estrutura do firmware é desactivada.

Padrão: [Não receber]

Violação entrada de senha

O administrador do equipamento pode especificar isso.

Se o número de pedidos de autenticação exceder o número especificado na definição, o sistema identifica o acesso como um ataque de senha. O acesso é registrado no Log de acesso e os dados do log são enviados para o administrador do equipamento por e-mail.

Se "Máx de acessos permitidos" estiver definido como [0], os ataques de senhas não são detectados.

- Máx de acessos permitidos

  Especifique o número máximo de tentativas de autenticação permitido.

  Utilize as teclas numéricas para especificar o valor entre "0" e "100" e, em seguida, pressione [#].

  Predefinição: [30]

- Hora da medição

Especifique o intervalo entre as tentativas repetidas de autenticação que resultam em falhas de autenticação. Quando o tempo de medição é ultrapassado, os registros de tentativas de autenticação são apagados.

Utilize as teclas numéricas para especificar o valor entre "1" e "10" e, em seguida, pressione [#].

Predefinição: [5]

- Dependendo dos valores especificados nas definições de [Máx de acessos permitidos] e [Hora da medição], é possível receber com frequência emails de detecção de violação.
- Se receber frequentemente emails de detecção de violação, verifique o conteúdo e reveja os valores das definições.

Defin. segurança em caso de violação do acesso

O administrador do equipamento.

Ao fazer o login no equipamento através de uma aplicação de rede, um usuário pode ser bloqueado por engano porque o número de tentativas de autenticação do usuário não corresponde ao número de tentativas especificadas no equipamento.

Por exemplo, o acesso pode ser negado quando um trabalho de impressão para vários conjuntos de páginas é enviado a partir de uma aplicação.

Se selecionar [Ligado] em "Defin. segurança em caso de violação do acesso", é possível evitar tais erros de autenticação.

- Ligado
    - Tempo negação p/violaç acess.

      Especifique quantos acessos de usuários são permitidos.

      Utilize as teclas numéricas para especificar o valor entre "0" e "60" e, em seguida, pressione [#].

      Predefinição: [15]
    - Limite host usuár gerenc

      Especifique quantas contas de usuários podem ser gerenciadas em "Definição de Segurança para Violação de Acesso".

      Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, pressione [#].

      Predefinição: [200]
    - Limite host entr senha

      Especifique quantas senhas podem ser gerenciadas em "Def de segurança para violação de acesso".

Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, pressione [#].

Predefinição: [200]

- Interv monitor de status

  Especifique o intervalo de monitoração de "Limite host usuár gerenc e "Limite host entr senha".

  Utilize as teclas numéricas para especificar o valor entre "1" e "10" e, em seguida, pressione [#].

  Predefinição: [3]

- Desligado

Padrão: [Desligado]

Violação acesso ao disp

O administrador do equipamento pode especificar isso.

Se o número de pedidos de login ultrapassa o número especificado na definição, o sistema identifica o acesso como uma violação de acesso. O acesso é registrado no Log de acesso e os dados do log são enviados para o administrador do equipamento por e-mail. Além disso, é mostrada uma mensagem no painel de controle e no Web Image Monitor.

Se "Máx de acessos permitidos" estiver definido como [0], as violações de acesso não são detectadas.

Em "Tempo de atraso autenticação", é possível especificar o tempo de atraso da resposta aos pedidos de login para evitar que o sistema fique indisponível quando é detectada uma violação de acesso.

Em "Limite host acessos simultâneos", é possível especificar o número máximo de hosts que acessam o equipamento de cada vez. Se o número de acessos simultâneos exceder o número especificado na definição, o monitoramento ficará indisponível e o status do monitoramento do equipamento será registrado no log.

- Máx de acessos permitidos

  Especifique o número máximo de tentativas de acesso permitido.

  Utilize as teclas numéricas para especificar o valor entre "0" e "500" e, em seguida, pressione [#].

  Predefinição: [100]

- Hora da medição

  Especifique o intervalo entre acessos excessivos. Quando o tempo de medição é ultrapassado, os registros de acessos excessivos são apagados.

  Utilize as teclas numéricas para especificar o valor entre "10" e "30" e, em seguida, pressione [#].

  Predefinição: [10]

- Tempo atraso autentic

  Especifique o tempo de atraso para autenticação quando é detectada uma violação de acesso.

  Utilize as teclas numéricas para especificar o valor entre "0" e "9" e, em seguida, pressione [#].

  Predefinição: [3]

- Limite host acessos simultân

  Especifique o número de tentativas de autenticação aceitável quando as autenticações são atrasadas devido a uma violação de acesso.

  Utilize as teclas numéricas para especificar o valor entre "50" e "200" e, em seguida, pressione [#].

  Predefinição: [200]

- Dependendo dos valores especificados das definições de [Máx de acessos permitidos] e [Hora da medição], é possível receber com frequência emails de detecção de violação.
- Se receber frequentemente emails de detecção de violação, verifique o conteúdo e reveja os valores das definições.

Outras funções de segurança

Esta seção explica as definições para prevenção de vazamento de informações.

São explicadas também as funções restritas quando a autenticação de usuário é ativada.

Função de scanner

Imprimir e excluir o diário do scanner

Quando a autenticação de usuário estiver ativada, "Imprimir e excluir o jornal do scanner" é ajustado automaticamente para [Não imprimir: Desativar envio] para evitar a impressão automática de informação pessoal no histórico de transmissão/entrega. Neste caso, o scanner é desativado automaticamente quando o histórico do jornal ultrapassa 250 transmissões ou entregas. Quando tal acontecer, seleccione [Imprimir jornal do scanner] ou [Eliminar jornal do scanner]. Para imprimir o diário scanner automaticamente, defina [Imprimir e excluir tudo] para "Imprimir e excluir diário scanner".

Para mais detalhes, consulte Digitalizar.

Função de scanner WSD

A função de scanner WSD é automaticamente desativada quando a autenticação de usuário é especificada. Mesmo que esteja automaticamente desativada, ela pode ser ativada em "Definições iniciais" disponíveis no Monitor imag da Web.

Para mais detalhes, consulte "Preparando-se para usar o Scanner WSD (Tipo Push)" e "Preparando-se para usar o Scanner WSD (Tipo Pull)", em Digitalizar.

Estado do sistema

Pressionar a tecla [Verificar status] no painel de controle permite verificar o status e as definições atuais da máquina. Se a autenticação do administrador tiver sido especificada, [Inform de end da máq] será exibido em[Inf de manut/consulta/máq] apenas se você tiver efetuado login como administrador.

Verificar validade do Firmware

Quando o equipamento é iniciado, esta função é usada para verificar se o firmware está válido.

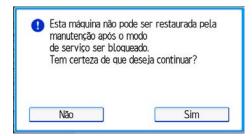
Caso ocorra erro durante o processo de verificação, um erro de verificação é exibido no painel de controle.

Observe que isso pode ser verificado também no Web Image Monitor após o início do equipamento. Caso ocorra um erro em um processo de verificação do Web Image Monitor, o Web Image Monitor não pode ser usado. Neste caso, verifique o painel de controle.

Restringir uma operação técnica do cliente

Você pode restringir o acesso do técnico do cliente ao modo de serviço.

Um engenheiro do cliente usa o modo serviço para inspeção ou reparo. Ao definir "Bloqueio do modo de serviço" como [Ligado], o modo de serviço não poderá ser usado, a não ser que o administrador do equipamento faça o login e cancele o bloqueio do modo de serviço para permitir que o técnico de um cliente opere a máquina para inspeção ou reparo. Isto garante que a inspeção e reparo podem ser realizadas sob a supervisão do administrador do equipamento.

1. **Faça login como administrador do equipamento no painel de controle.**
2. **Pressione [Definições do sistema].**
3. **Pressione [Ferramentas admin].**
4. **Pressione [▼Próximo] duas vezes.**
5. **Pressione [Bloqueio do modo de serviço].**
6. **Pressione [Ligado] e, em seguida, [OK].**
7. **Pressione [Sim].**

8. **Faça logout.**

Informações Adicionais para Segurança Avançada

Esta secção explica as definições que pode configurar para reforçar a segurança do equipamento.

Definições que pode configurar utilizando o painel de controlo

Utilize o painel de controlo para configurar as definições de segurança indicadas na seguinte tabela.

Configurações do sistema

Guia	Item	Definição
Definições de timer	Timer de logout automático	Ligado: 180 segundos ou menos. Consulte Pág. 61 "Logout automático".
Ferramentas de admin	Gerenciamento de autenticação de usuário	Selecione [Aut. básica], e ajuste a "Autentic de trab de impressora" em [Inteiro]. Consulte Pág. 34 "Autenticação básica".
Ferramentas de admin	Gestão de autenticação do administrador→Gestão de usuários	Selecione [Ligado], e em seguida ajuste [Ferramentas de admin] para "Definições disponíveis". Consulte Pág. 14 "Configurar a autenticação de administrador".
Ferramentas de admin	Gerenciam. de máquina→ Gerenciam. de máquina	Selecione [Ligado] e, em seguida, selecione cada uma das "Definições disponíveis". Consulte Pág. 14 "Configurar a autenticação de administrador".
Ferramentas de admin	Gestão de autenticação do administrador→ Gerenciamento de rede	Selecione [Ligado], e em seguida ajuste [Definições de interface], [Transf de arquivos], e [Ferramentas de admin] para "Definições disponíveis". Consulte Pág. 14 "Configurar a autenticação de administrador".

Guia	Item	Definição
Ferramentas de admin	Gestão de autenticação do administrador→Gestão de arquivos	Selecione [Ligado], e em seguida ajuste [Ferramentas de admin] para "Definições disponíveis". Consulte Pág. 14 "Configurar a autenticação de administrador".
Ferramentas de admin	Segurança estendida→ Definições por SNMPv1, v2	Proibir Consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".
Ferramentas de admin	Segurança estendida→ Chave criptografia do driver: Nível cript	AES Consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".
Ferramentas de admin	Segurança estendida→ Autenticar tarefa atual	Privilégio de acesso Consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".
Ferramentas de admin	Segurança estendida→ Política de senha	"Definição de complexidade": Nível 1 ou mais, "Nº mínimo de caracteres ": 8 ou mais Consulte Pág. 250 "Especificar as Funções de Segurança Avançadas".
Ferramentas de admin	Nível de segurança de rede	Nível 2 Para obter o status do equipamento através do driver da impressora ou do Web Image Monitor, ative "SNMP" no Web Image Monitor. Consulte Pág. 114 "Especificar Níveis de segurança da rede".
Ferramentas de admin	Bloqueio do modo de serviço	Ligado Consulte Pág. 259 "Restringir uma operação técnica do cliente".

Guia	Item	Definição
Ferramentas de admin	Definições de criptografia de dados da máquina	Selecione [Criptografar] e, em seguida, selecione [Todo os dados] para "Transfira todos os dados, somente os dados do sistema de arquivos (sem formatação) ou formate todos os dados ". Se [Criptografar] já estiver selecionado, não são necessárias mais definições de criptografia. Consulte Pág. 89 "Criptografar dados no equipamento".

Recursos de scanner

Guia	Item	Definição
Definições Iniciais	Proteger menu	Nível 2 Consulte Pág. 68 "Especificar a definição Proteger menu".

- A definição SNMP pode ser especificada em [SNMP] sobre [Configuração] no Web Image Monitor.

Definições que pode configurar utilizando o Web Image Monitor

Utilize o Web Image Monitor para configurar as definições de segurança apresentadas na tabela seguinte.

Gerenciamento do dispositivo→Configuração

Categoria	Item	Definição
Definições do dispositivo→Logs	Coletar logs de trabalho	Ativo
Definições do dispositivo→Logs	Coletar logs de acesso	Ativo

Categoria	Item	Definição
Segurança→ Política de bloqueio do usuário	Bloqueio	Ativo Para mais informações, consulte Pág. 59 "Função Bloqueio de usuário".
Segurança→ Política de bloqueio do usuário	Número de tentativas antes do bloqueio	5 vezes ou menos. Para mais informações, consulte Pág. 59 "Função Bloqueio de usuário".
Segurança→ Política de bloqueio do usuário	Timer de liberação de bloqueio	Defina para [Ativo] ou [Inativo]. Quando definir para [Ativo], ajuste o temporizador de cancelamento de bloqueio para 60 minutos ou mais. Para mais informações, consulte Pág. 59 "Função Bloqueio de usuário".
Segurança→ Política de bloqueio do usuário	Bloquear usuário para	Ao ajustar "Timer de liberação de bloqueio" para [Ativo], ajuste o timer de liberação de bloqueio em 60 minutos ou mais. Para mais informações, consulte Pág. 59 "Função Bloqueio de usuário".
Rede→SNMPv3	Função SNMPv3	Inativo Para usar as funções SNMPv3, ajuste a "Função SNMPv3" em [Ativo], e ajuste a "Permitir comunicação SNMPv3" em [Somente criptografia]. Uma vez que SNMPv3 garante a autenticação para cada pacote, o log de logins será desativado assim que SNMPv3 for ativado.
Segurança→ Segurança de rede	FTP	Inativo Antes de especificar esta definição, ajuste o "Nível de segurança da rede" no painel de controle em [Nível 2].
Segurança	S/MIME	"Algoritmo de criptografia": AES-128 bits, AES-256 bits ou 3DES-168 bits Você deve registrar o certificado de usuário para utilizar o S/MIME.

Gerenciamento do dispositivo

Categoria	Item	Definição
Address Book→ Entrada detalhada→ Adicionar usuário/Alterar→ E-mail	Certificado de usuário	Você deve registrar o certificado de usuário para utilizar o S/MIME.

Nota

- O administrador deve indicar o nível de grau que pode ser especificado para o algoritmo de criptografia.
- Para saber como especificar um algoritmo de criptografia e registrar um certificado de usuário, consulte Pág. 130 "Configurar S/MIME".

Definições que pode configurar quando o IPsec está disponível/indisponível

7

Toda a comunicação de e para equipamentos em que o IPsec está ativo é criptografada.

Se a sua rede suportar IPsec, recomendamos que a ative.

Definições que você pode configurar quando o IPsec está disponível

Se o IPsec estiver disponível, configure as definições indicadas na tabela seguinte para melhorar a segurança dos dados que circulam na sua rede.

Definições do painel de controlo

Configurações do sistema

Guia	Item	Definição
Definições de interface	IPsec	Ativo
Definições de interface	Permitir comunicação SSL/ TLS	Somente texto cifrado

Definições do Web Image Monitor

Gerenciamento do dispositivo→Configuração

Categoria	Item	Definição
Segurança→ IPsec→ Definições de troca automática de chave de criptografia	Editar→Nível de segurança	Definição concluída

Definições que pode configurar quando o IPsec não está disponível

Se o IPsec não estiver disponível, configure as definições apresentadas na tabela seguinte para melhorar a segurança dos dados que circulam na sua rede.

Definições do painel de controlo

Configurações do sistema

Guia	Item	Definição
Definições de interface	IPsec	Inativo
Definições de interface	Permitir comunicação SSL/ TLS	Somente texto cifrado

- É possível definir "IPsec" e "Permitir comunicação SSL/TLS" utilizando o Web Image Monitor.

Proteger dados quando o IPsec não está disponível

Os seguintes procedimentos aprimoram a segurança dos dados do usuário quando IPsec não está disponível.

Os administradores devem instruir os usuários para executar estes procedimentos.

Impressora

- Imprimir com protocolos que suportam criptografia:

  Para utilizar as funções de impressora, especifique sftp como o protocolo, ou especifique IPP e ative SSL/TLS.

  Para obter mais informações sobre definições de IPP, consulte Printer Driver Installation Guide.

Para mais informações sobre definições de SSL/TLS, consulte Pág. 124 "Configurar definições SSL/TLS".

Scanner

- Enviar o endereço URL de arquivos armazenados

  Envie a URL dos arquivos digitalizados para os destinos configurando [Definições de envio] em [Recursos de scanner], em vez de enviar os próprios arquivos digitalizados. Para mais informações, consulte Scan.

- Gerenciar arquivos usando o Web Image Monitor

  Utilize o Web Image Monitor através da sua rede para visualizar, apagar, enviar e transferir ficheiros digitalizados.

- Função de autenticação S/MIME

  Ao enviar os arquivos digitalizados anexados ao email, proteja-os aplicando um certificado S/MIME. Para isso, configure as definições de "Segurança" antes de enviar os arquivos. Para obter informações sobre como enviar e-mail do scanner, consulte Scan.

- Para mais informações sobre ativação e desativação do IPsec utilizando o painel de controle, consulte Connecting the Machine/ System Settings.
- Para saber como especificar a definição IPsec via Web Image Monitor, consulte Pág. 138 "Configurar definições IPsec".

8. Solução de problemas

Este capítulo descreve o que fazer se o equipamento não funcionar correctamente.

Se aparecer uma mensagem

Este capítulo explica como tratar de problemas se uma mensagem aparecer no ecrã durante a autenticação do utilizador.

Se uma mensagem não mostrada abaixo for exibida, siga as orientações da mensagem para resolver o problema.

"Você não tem privilégios para usar essa função."

Os privilégios para utilizar a função não foram especificados.

Se isto for exibido durante o uso de uma função:

- A função não está especificada na definição de gerenciamento do Catálogo de endereços.
- O administrador de usuários deve decidir se os privilégios para utilizar a função devem ser atribuídos adicionalmente.

Se isso aparecer ao especificar a definição de um equipamento:

- O administrador varia de acordo com as definições do equipamento que o usuário deseja especificar.
- Usando a lista de definições, o administrador responsável pelas definições que os usuários desejam usar no equipamento deve decidir se deve atribuir os privilégios de uso da função.

8

"Falha na autenticação.".

As causas de falhas de autenticação variam e são indicadas com códigos de erros.

Para mais informações, consulte Pág. 269 "Se aparecer um código de erro".

"A autenticação de administrador para gerenciamento de usuário deve ser definida como ligada antes que se possa fazer essa seleção. "

Os privilégios de administrador do usuário não foram ativados em [Gerenciamento de autenticação de administrador].

- Para especificar as autenticações Básica, Windows ou LDAP, é necessário ativar primeiro os privilégios do administrador de usuários em [Gerenciamento de autenticação de administrador].

Para mais informações, consulte Pág. 14 "Configurar a autenticação de administrador".

"Os arquivos selecionados continham arquivos sem privilégios de acesso. Apenas arquivos com privilégios de acesso serão excluídos."

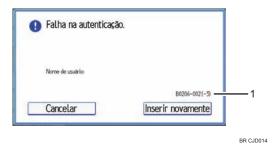
Foi feita uma tentativa de apagar arquivos sem a autoridade para fazê-lo.

- O proprietário ou administrador do arquivo podem excluir os arquivos. Para excluir um arquivo para o qual não tem autorização para excluir, contate o proprietário ou o administrador do arquivo.

- Se aparecer uma mensagem de chamada de assistência, contate a assistência técnica.

Se aparecer um código de erro

Quando houver falha na autenticação, a mensagem "Falha na autenticação. " será exibida com um código de erro. As listas a seguir fornecem soluções para cada código de erro. Se um código de erro não aparece nas listas abaixo, anote-o e entre em contato com a assistência técnica.

Posição de exibição do código de erro

1. **Código de erro**

   Aparece um código de erro.

Autenticação básica

B0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador iniciou sessão no equipamento e, em seguida, tente novamente.

B0104-000

Não foi possível desencriptar a palavra-passe.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida correctamente.

- A [DES] ou a [AES] é selecionada para "Chave criptografia do driver: Nível cript".

  Você pode disponibilizar o acesso especificando a chave de criptografia do driver.

- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está correctamente especificado no driver.

B0206-002 : Caso 1

Ocorreu um erro com o nome de utilizador ou a palavra-passe de início de sessão.

- Certifique-se de que o nome de utilizador e a palavra-passe de início de sessão estão introduzidos correctamente e, em seguida, inicie a sessão.

B0206-002 : Caso 2

O usuário tentou a autenticação em um aplicativo na tela "Definições do sistema", mas apenas o administrador tem privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

B0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes caracteres proibidos.
- Se o nome da conta foi inserido erradamente, insira o nome correto e faça o login novamente.

B0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

B0208-000 / B0208-002

A conta está bloqueada porque o número permitido de tentativas de autenticação chegou ao máximo.

- Peça ao administrador de utilizadores para desbloquear a conta.

Autenticação Windows

W0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador possui sessão iniciada no equipamento e, em seguida, tente novamente.

W0104-000

Não foi possível criptografar uma senha.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida correctamente.
- A [DES] ou a [AES] é selecionada para "Chave criptografia do driver: Nível cript".

  Você pode disponibilizar o acesso especificando a chave de criptografia do driver.
- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está correctamente especificado no driver.

W0206-002

O usuário tentou a autenticação em um aplicativo na tela "Definições do sistema", mas apenas o administrador tem privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

W0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes caracteres proibidos.
- Se o nome da conta foi inserido erradamente, insira o nome correto e faça o login novamente.

W0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

W0208-000 / W0208-002

A conta está bloqueada porque o número permitido de tentativas de autenticação chegou ao limite.

- Peça ao administrador de utilizadores para desbloquear a conta.

W0400-102

A autenticação Kerberos falhou porque o servidor não está funcionando corretamente.

- Certifique-se de que o servidor está a funcionar adequadamente.

W0400-200

Devido ao significativo número de tentativas de autenticação, todos os recursos estão ocupados.

- Aguarde alguns minutos e tente novamente.

W0400-202 : Caso 1

As definições SSL no servidor de autenticação e no equipamento não correspondem.

- Certifique-se de que as definições SSL no servidor de autenticação e no equipamento correspondem.

W0400-202 : Caso 2

O utilizador introduziu sAMAccountName no nome de utilizador para iniciar sessão.

- Se um utilizador introduzir sAMAccountName como nome de utilizador de início de sessão, o ldap_bind falha num ambiente de domínio/subdomínio. Ao invés, utilize o UserPrincipleName (UPN) como nome de início de sessão.

W0406-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes caracteres proibidos.
- Se o nome da conta foi inserido incorretamente, insira o nome correto e faça login outra vez.

W0406-101

A autenticação não pode ser concluída devido ao número significante de tentativas de autenticação.

- Aguarde alguns minutos e tente novamente.
- Se a situação não melhorar, certifique-se se não está ocorrendo um ataque de autenticação.
- Notifique o administrador da mensagem da tela por email e verifique se no registro do sistema há sinais de ataque potencial de autenticação.

W0406-107: Caso 1

O formato UserPrincipleName (UPN) (utilizador@nomedomínio.xxx.com) está a ser utilizado para o nome de utilizador de início de sessão.

- O grupo do utilizador não pode ser obtido se o formato NomePrincipalUtilizador (utilizador@nomedomínio.xxx.com) for utilizado.
- Utilize "NomeContasAM(utilizador)" para iniciar a sessão, porque esta conta permite obter o grupo do utilizador.

W0406-107: Caso 2

As definições actuais não permitem a recuperação do grupo.

- Certifique-se de que o âmbito do grupo de utilizadores está definido como "Grupo Global" e que o tipo de grupo está definido como "Segurança" nas propriedades do grupo.
- Certifique-se de que a conta foi adicionada ao grupo de utilizadores.
- Certifique-se de que o nome do grupo de utilizadores registado no equipamento e o nome do grupo no DC (domain controller) são exactamente os mesmos. O DC distingue maiúsculas e minúsculas.
- Certifique-se de que "Use inf de autor no login" foi especificado em "Inform Aut." na conta de usuário registrada no equipamento.
- Se existir mais do que um DC, certifique-se de que uma relação confidencial foi configurada entre cada DC.

W0406-107 : Caso 3

Não é possível resolver o nome do domínio.

- Certifique-se de que o DNS/WINS esteja especificado no nome de domínio "Definições de interface".

W0406-107: Caso 4

Não é possível estabelecer ligação ao servidor de autenticação.

- Certifique-se de que a ligação ao servidor de autenticação é possível.
- Use o "Comando ping" em "Definições de interface" para checar a conexão.

W0406-107: Caso 5

Ocorreu um erro com o nome ou a palavra-passe de início de sessão.

- Certifique-se de que o utilizador está registado no servidor.
- Utilize um nome de utilizador e uma palavra-passe de início de sessão.

W0406-107 : Caso 6

Ocorreu um erro de nome de domínio.

- Certifique-se de que o nome de domínio da autenticação Windows está correctamente especificado.

W0406-107: Caso 7

Não é possível resolver o nome do domínio.

- Especifique o endereço IP no nome de domínio e confirme que a autenticação foi bem sucedida.

  Se a autenticação tiver sido bem sucedida:

  - Se o nome de domínio de nível superior for especificado no nome de domínio (como nomedomínio.xxx.com), certifique-se de que DNS está especificado em "Definições de interface".
  - Se um nome de domínio NetBIOS for especificado no nome de domínio (como NOMEDOMÍNIO), certifique-se de que o WINS esteja especificado nas "Defs de interface".

  Se a autenticação não tiver sido bem sucedida:

  - Certifique-se de que Restringir LM/NTLM não está definido em "Política de Segurança do Controlador do Domínio" ou "Política de Segurança do Domínio".
  - Certifique-se de que as portas para a firewall de controlo de domínio e a firewall no equipamento para o caminho da ligação de controlo do domínio estão abertas.
- Se o firewall do Windows estiver ativado, crie uma regra de firewall nas "Definições avançadas" do firewall do Windows para autorizar as portas 137 e 139.
- Na janela Propriedades para "Conexões de rede", abra as propriedades de TCP/IP. Em seguida, clique nas definições detalhadas, WINS, assinale a caixa "Activar NetBIOS sobre TCP/IP" e defina o número 137 como "Aberto".

W0406-107: Caso 8

A autenticação Kerberos falhou.

- As definições da autenticação Kerberos não estão correctamente configuradas.

8

Certifique-se de que o nome do realm, o nome KDC (Key Distribution Center) e o nome de domínio estejam devidamente especificados.

- Os tempos do KDC e do equipamento não correspondem.

  A autenticação falhará se a diferença entre o tempo do KDC e o do equipamento for superior a 5 minutos. Certifique-se de que os tempos são coincidentes.

- A autenticação do Kerberos falhará se o nome do realm for especificado em minúsculas. Certifique-se de que o nome do realm é especificado em maiúsculas.
- A autenticação Kerberos falhará se a recuperação automática para o KDC falhar.

  Peça à assistência técnica para certificar-se de que as definições de recuperação do KDC estão definidas para "recuperação automática".

  Se a recuperação automática não estiver a funcionar correctamente, mude para recuperação manual.

W0409-000

Esgotou-se o tempo da autenticação porque o servidor não respondeu.

- Verifique a configuração de rede ou as definições no servidor de autenticação.

W0511-000 / W0517-000

O nome de início de sessão do servidor de autenticação é igual a um nome de utilizador já registado no equipamento. (Os nomes são identificados pelo atributo único especificado nas definições de autenticação do LDAP.)

- Exclua o nome antigo duplicado ou mude o nome de login.
- Se o servidor de autenticação tiver sido alterado recentemente, apague o nome antigo no servidor.

W0606-004

A autenticação falhou porque o nome do usuário contém palavras que não podem ser usadas pelos usuários gerais.

- Não utilize "other", "admin", "supervisor" ou "HIDE*" em contas de utilizadores gerais.

W0607-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

W0612-005

A autenticação falhou porque não é possível registar mais utilizadores. (O número de usuários registrados no Catálogo de endereços chegou ao máximo.)

- Peça ao administrador de utilizadores para apagar contas de utilizadores não utilizadas no Livro de Endereços.

W0707-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

W09XX-019

Falha no registro automático do usuário no servidor ao autenticar o acesso do cliente usando a função Gerenciamento central do Catálogo de endereços.

- Verifique a conexão de rede entre o cliente e o servidor.
- Não é possível registrar usuários durante a edição do Catálogo de endereços.

Autenticação LDAP

L0103-000

Ocorreu uma operação TWAIN durante a autenticação.

- Certifique-se de que nenhum outro utilizador possui sessão iniciada no equipamento e, em seguida, tente novamente.

L0104-000

Não foi possível criptografar uma senha.

- Ocorreu um erro de palavra-passe.

  Certifique-se de que a palavra-passe foi introduzida correctamente.
- A [DES] ou a [AES] é selecionada para "Chave criptografia do driver: Nível cript".

  Você pode disponibilizar o acesso especificando a chave de criptografia do driver.
- Ocorreu um erro de código de encriptação do driver.

  Certifique-se de que o código de encriptação está correctamente especificado no driver.

L0206-002

Um usuário tentou fazer uma autenticação a partir de um aplicativo na tela "Definições do sistema", onde apenas o administrador tenha privilégios de autenticação.

- Apenas o administrador possui privilégios para iniciar sessão neste ecrã.
- Inicie a sessão como um utilizador geral a partir do ecrã de início de sessão da aplicação.

L0206-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes caracteres proibidos.
- Se o nome da conta foi inserido erradamente, insira o nome correto e faça o login novamente.

L0207-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

L0208-000 / L0208-002

A conta está bloqueada porque o número permitido de tentativas de autenticação chegou ao máximo.

- Peça ao administrador de utilizadores para desbloquear a conta.

L0307-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

L0400-210

Falhou a obtenção de informações de utilizador na procura LDAP.

- As condições de pesquisa do atributo de login podem não estar especificadas ou as informações de pesquisa especificadas não estão acessíveis.
- Certifique-se de que o atributo do nome de início de sessão está especificado correctamente.

L0406-003

Ocorreu um erro de autenticação porque o nome de utilizador contém um espaço, dois pontos (:) ou aspas (").

- Volte a criar a conta se o nome da conta contiver algum destes caracteres proibidos.
- Se o nome da conta foi inserido erradamente, insira o nome correto e faça o login novamente.

L0406-200

A autenticação não pode ser concluída devido ao número significante de tentativas de autenticação.

- Aguarde alguns minutos e tente novamente.
- Se a situação não melhorar, certifique-se se não está ocorrendo um ataque de autenticação.
- Notifique o administrador da mensagem da tela por email e verifique se no registro do sistema há sinais de ataque potencial de autenticação.

L0406-201

A autenticação está desactivada nas definições do servidor LDAP.

- Altere as definições do servidor LDAP nas ferramentas do administrador, em "Definições do sistema".

L0406-202 / L0406-203 : Caso 1

Existe um erro nas definições de autenticação LDAP, no servidor LDAP ou na configuração de rede.

- Certifique-se de que um teste da ligação é bem sucedido com a configuração actual do servidor LDAP.

Caso a conexão falhe, pode ter havido um erro nas definições da rede.

Verifique o nome do domínio ou as definições DNS em "Definições de interface".

- Certifique-se de que o servidor LDAP é especificado correctamente nas definições da autenticação LDAP.
- Certifique-se de que o atributo do nome de início de sessão é introduzido correctamente nas definições de autenticação LDAP.
- Certifique-se de que as definições SSL são suportadas pelo servidor LDAP.

L0406-202 / L0406-203 : Caso 2

Ocorreu um erro com o nome de utilizador ou a palavra-passe de início de sessão.

- Certifique-se de que o nome de utilizador e a palavra-passe de início de sessão estão introduzidos correctamente.
- Certifique-se de que um nome de início de sessão utilizável está registrado no equipamento.

  A autenticação falhará nos casos seguintes.

  Se o nome de utilizador de início de sessão contiver um espaço, dois pontos (:), ou aspas (").

  Se o nome de utilizador de início de sessão exceder os 128 bytes.

L0406-202 / L0406-203 : Caso 3

Existe um erro no método de encriptação simples.

- A autenticação falhará se a palavra-passe ficar em branco no modo de autenticação simples.

  Para permitir senhas em branco, contate seu representante técnico.

- No modo de autenticação simples, o DN do nome de utilizador de início de sessão obtém-se na conta do utilizador.

  A autenticação falha se não se conseguir obter o DN.

  Certifique-se de que não existam erros no nome do servidor, nome ou senha de usuário ou nas informações inseridas no filtro de pesquisa.

L0406-204

A autenticação Kerberos falhou.

- As definições da autenticação Kerberos não estão correctamente configuradas.

  Certifique-se de que o nome do realm, o nome do KDC (Key Distribution Center) e o nome do domínio de apoio estão especificados correctamente.

- Os tempos do KDC e do equipamento não correspondem.

  A autenticação falhará se a diferença entre o tempo do KDC e o do equipamento for superior a 5 minutos. Certifique-se de que os tempos são coincidentes.

- A autenticação do Kerberos falhará se o nome do realm for especificado em minúsculas. Certifique-se de que o nome do realm é especificado em maiúsculas.

L0409-000

Esgotou-se o tempo da autenticação porque o servidor não respondeu.

- Contacte o administrador do servidor ou da rede.
- Se a situação não melhorar, contate a assistência técnica.

L0511-000

O nome de início de sessão do servidor de autenticação é igual a um nome de utilizador já registado no equipamento. (Os nomes são identificados pelo atributo único especificado nas definições de autenticação LDAP.)

- Exclua o nome antigo duplicado ou mude o nome de login.
- Se o servidor de autenticação tiver sido alterado recentemente, apague o nome antigo no servidor.

L0606-004

A autenticação falhou porque o nome do usuário contém palavras que não podem ser usadas pelos usuários gerais.

- Não utilize "other", "admin", "supervisor" ou "HIDE*" em contas de utilizadores gerais.

L0607-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

L0612-005

A autenticação falhou porque não é possível registar mais utilizadores. (O número de usuários registrados no Catálogo de endereços chegou ao máximo.)

- Peça ao administrador de utilizadores para apagar contas de utilizadores não utilizadas no Livro de Endereços.

L0707-001

Ocorreu um erro de autenticação porque o livro de endereços está a ser utilizado noutro local.

- Aguarde alguns minutos e tente novamente.

L09XX-019

Falha no registro automático do usuário no servidor ao autenticar o acesso do cliente usando a função Gerenciamento central do Catálogo de endereços.

- Verifique a conexão de rede entre o cliente e o servidor.
- Não é possível registrar usuários durante a edição do Catálogo de endereços.

Se não for possível operar o equipamento

Se as seguintes condições surgirem enquanto os utilizadores estiverem a utilizar o equipamento, disponibilize instruções sobre como lidar com elas.

Problema	Causa	Solução
Não é possível realizar o seguinte: • Imprimir com o driver de impressão • Ligar com o driver TWAIN	A autenticação do usuário foi rejeitada.	Se estiver utilizando a autenticação do Windows ou LDAP, verifique o nome de usuário e o nome de login em uso com o administrador da rede. Confirme com o administrador de utilizadores se utilizar a autenticação básica.
Não é possível realizar o seguinte: • Imprimir com o driver de impressão • Ligar com o driver TWAIN	O código de encriptação especificado no driver não corresponde ao código de encriptação do driver do equipamento.	Especifique o código de encriptação do driver registado no equipamento. Para mais informações, consulte Pág. 162 "Especificar uma chave de criptografia de driver".
Não é possível ligar ao driver TWAIN.	A conta, senha e algoritmo de criptografia de SNMPv3 não correspondem às definições especificadas neste equipamento.	Especifique a conta, palavra--passe e o algoritmo de encriptação do SNMPv3 registado no equipamento utilizando as ferramentas de ligação de rede.
Não é possível autenticar com o driver TWAIN.	Outro usuário fez o login no equipamento.	Aguarde que o utilizador encerre a sessão.
Não é possível autenticar com o driver TWAIN.	A autenticação está demorando devido às condições operacionais.	Certifique-se de que a definição do servidor LDAP está correcta. Certifique-se de que as definições de rede estão correctas.

8

Problema	Causa	Solução
Não é possível autenticar com o driver TWAIN.	A autenticação não é possível enquanto o equipamento estiver a editar os dados do livro de endereços.	Aguarde que a edição dos dados do livro de endereços esteja concluída.
Após iniciar o "Catálogo de endereços" em Device Manager NX e inserir o nome de usuário de login e a senha corretos, é exibida uma mensagem informando que foi um inserida uma senha incorreta.	A "Chave criptografia do driver: Nível cript" não está definida corretamente. Ou então, "SSL/ TLS" foi ativado mesmo sem que o certificado necessário estivesse instalado no computador.	Defina "Chave de criptografia de driver:Grau de criptografia" como [Criptografia simples]. Em alternativa, active "SSL/TLS", instale o certificado do servidor no equipamento e, em seguida, instale o certificado no computador. Para obter mais informações, consulte Pág. 250 "Especificar as Funções de Segurança Avançadas" e Pág. 124 "Configurar definições SSL/ TLS".
Não é possível encerrar a sessão utilizando as funções do copiador ou do scanner.	O original não foi completamente digitalizado.	Quando o original tiver sido completamente varrido, pressione [#], remova o original e efetue logoff.
"Dest progr " não é exibido na tela do scanner para especificação de destinos.	"Restringir adição de destinos de usuários" está definido como [Ligado] em "Segurança estendida", portanto, só o administrador do usuário pode registrar destinos no Catálogo de endereços na tela do scanner.	O registro deve ser executado pelo administrador do usuário.

8

Problema	Causa	Solução
Não é possível enviar e-mails a partir do scanner. Da mesma forma: • Não é possível selecionar um endereço. • Não é possível especificar uma assinatura. • Não é possível armazenar os dados em uma mídia.	As opções abaixo são possíveis causas: • O período de validade do certificado do usuário (certificado de destino) expirou. • O período de validade do certificado do dispositivo (S/MIME) expirou. • O certificado do dispositivo (S/MIME) não existe ou é inválido. • O período de validade do certificado do dispositivo (PDF ou PDF/A com assinatura digital) expirou. • O certificado do dispositivo (PDF ou PDF/A com assinatura digital) não existe ou é inválido. • O endereço de e-mail do administrador está incorreto.	• Instale um certificado de usuário (certificado de destino). Um certificado de usuário (certificado de destino) pode ser instalado a partir do livro de endereço do Web Image Monitor. O certificado de usuário (certificado de destino) deve ser preparado antecipadamente. • Instale um certificado de dispositivo para S/MIME. • Instale um certificado de dispositivo para PDF ou PDF/A com assinatura digital. Para mais informações, consulte Pág. 119 "Proteger os caminhos de comunicação via certificado de dispositivo". • Especifique o endereço de e-mail do administrador. Para mais detalhes, consulte Conexão da máquina/Definições do sistema.

8

Problema	Causa	Solução
A autenticação do utilizador está desactivada; no entanto, os ficheiros guardados não aparecem.	A autenticação de usuário deve ter sido desativada sem ter selecionado "Todos os usuários" para acesso do usuário para arquivos armazenados.	Ative a autenticação do usuário novamente e selecione [Todos os usuários] como definição da permissão de acesso dos arquivos que deseja exibir. Para mais informações, consulte a Ajuda do Pág. 171 "Gerenciar arquivos armazenados" e Web Image Monitor .
A autenticação do utilizador está desactivada, mas os destinos especificados utilizando o equipamento não aparecem.	A autenticação do usuário foi desativada sem que a opção "Todos os usuários" fosse selecionada para "Proteger destino".	Ative a autenticação do usuário novamente e selecione [Todos os usuários] como definição da permissão de acesso dos destinos que deseja exibir. Para mais informações, consulte Pág. 85 "Proteger o Catálogo de endereços".
Não é possível imprimir quando a autenticação de utilizadores está activada.	A autenticação de utilizadores pode não ter sido especificada no driver de impressão.	Especifique a autenticação de utilizadores no driver de impressão. Para mais informações, consulte a Ajuda do driver de impressão.
[Concluir trabalho e limite] está selecionado em "Ação do equipamento quando é atingido o limite", mas o trabalho atual é cancelado antes de ser processado.	Dependendo do aplicativo que você estiver usando, o equipamento pode reconhecer um trabalho como vários trabalhos, cancelando o trabalho antes de ser processado.	Reponha a definição de utilização do volume de impressão para o utilizador, por exemplo, ao limpar o contador de utilização do volume de impressão e, em seguida, imprimir novamente. Para mais informações, consulte Pág. 81 "Redefinir os contadores de uso do volume de impressão".

8

Problema	Causa	Solução
Se tentar interromper um trabalho enquanto copia ou digitaliza, aparece um ecrã de autenticação.	Com este equipamento, pode encerrar a sessão enquanto copia ou digitaliza. Se tentar interromper uma cópia ou uma digitalização após ter encerrado a sessão, aparece um ecrã de autenticação.	Apenas o utilizador que executou um trabalho de cópia ou digitalização pode interromper o mesmo. Espere até a conclusão do trabalho ou verifique com o usuário quem executou o trabalho. O administrador do equipamento pode excluir trabalhos.
Depois de executar "Cript defs personaliz do usuár e cat end", a mensagem "Sair" não aparecerá apesar da longa espera.	A autenticação pode estar demorando porque muitos dos itens estão registrados no catálogo de endereços. Como alternativa, um arquivo pode estar corrompido ou o disco rígido pode estar defeituoso.	Se a tela ainda não foi atualizada mesmo depois de decorrido o tempo de "Som dados sist de arq", especificado de acordo com Pág. 89 "Criptografar dados no equipamento", entre em contato com o seu representante técnico.

8

9. Lista de privilégios de operações em definições

Este capítulo relaciona uma lista dos privilégios de operações para administradores e usuários para as definições do equipamento quando a função de autenticação de administradores e usuários está ativada.

Como ler

Significado dos tipos cabeçalhos

- Usuário

  O administrador de usuários possui privilégios para esta operação.

- Equip

  O administrador do equipamento possui privilégios para esta operação.

- N/W

  O administrador da rede possui privilégios para esta operação.

- Arquivo

  O administrador de arquivos possui privilégios para esta operação.

- Unset

  O usuário que fez login possui privilégios para esta operação.

  Para os casos em que nenhuma definição é selecionada em "Definições disponíveis" de [Gerenciamento de autenticação de administrador].

- Definido

  O usuário que fez login possui privilégios para esta operação.

  Estado quando são selecionada definições em "Definições disponíveis" de [Gerenciamento de autenticação de administrador].

- Nív.1

  Para os casos em que a definição [Proteção de menu] está definida como [Nível 1].

- Nív.2

  Para os casos em que a definição [Proteção de menu] está definida como [Nível 2].

Significado dos símbolos

R/W: Permissão para execução, alteração e leitura.

R: Permissão para leitura.

-: Sem permissão para execução, alteração e leitura.

Configurações do sistema

Quando a autenticação do administrador é especificada, as restrições às operações dos usuários variam de acordo com as configurações em "Definições disponíveis".

[Caract gerais]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Programar/Alterar/Excluir texto de usuário]	R	R/W	R	R	R/W	R
[Som das teclas do painel]	R	R/W	R	R	R/W	R
[Sinal sonoro de aquecimento]	R	R/W	R	R	R/W	R
[Monitor de contagem de cópias]	R	R/W	R	R	R/W	R
[Prioridade de função]	R	R/W	R	R	R/W	R
[Alocação da tecla de função]	R	R/W	R	R	R/W	R
[Prioridade de impressão]	R	R/W	R	R	R/W	R
[Timer de redefinição de função]	R	R/W	R	R	R/W	R
[Interv tempo entre tarefas de impr]	R	R/W	R	R	R/W	R
[Definição de cor de tela]	R	R/W	R	R	R/W	R
[Saída: Copiadora]	R	R/W	R	R	R/W	R
[Saída: Servidor de documentos]	R	R/W	R	R	R/W	R
[Saída: Impressora]	R	R/W	R	R	R/W	R
[Definição da bandeja de saída]	R	R/W	R	R	R/W	R
[Prioridade da band de papel: Copiadora]	R	R/W	R	R	R/W	R
[Priorid da band de papel: Impressora]	R	R/W	R	R	R/W	R
[Repetição de tecla]	R	R/W	R	R	R/W	R
[Elevação da mesa de originais ADF]	R	R/W	R	R	R/W	R
[Status sist/Temp exib list tarefas]	R	R/W	R	R	R/W	R
[Impressão intercalar]	R	R/W	R	R	R/W	R

9

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Indicador de status]	R	R/W	R	R	R/W	R
[Posição da dobra em Z]	R	R/W	R	R	R/W	R
[Posição de dobra simples]	R	R/W	R	R	R/W	R
[Posição de dobra de carta para fora]	R	R/W	R	R	R/W	R
[Posição de dobra de carta para dentro]	R	R/W	R	R	R/W	R
[Posição de dobra dupla paralela]	R	R/W	R	R	R/W	R
[Posição de dobra em portada]	R	R/W	R	R	R/W	R
[Teclado externo]	R	R/W	R	R	R/W	R
[Programar/alterar lista de dispositivos USB]	R	R/W	R	R	R/W	R
[Ajuste fino do corte de encadernação sem costura]	R	R/W	R	R	R/W	R
[ID compatível]	R	R/W	R	R	R/W	R

[Definições do timer]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Timer do modo de suspensão]	R	R/W	R	R	R/W	R
[Timer do modo de baixa energia]	R	R/W	R	R	R/W	R
[Timer de redefinição automát do sist]	R	R/W	R	R	R/W	R
[Timer redef aut do servidor de copiadora/doc]	R	R/W	R	R	R/W	R
[Timer de redefin aut da impressora]	R	R/W	R	R	R/W	R
[Timer de redefinição aut do scanner]	R	R/W	R	R	R/W	R
[Definir data]	R	R/W	R	R	R/W	R
[Definir hora]	R	R/W	R	R	R/W	R
[Timer de logout automático]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Modo desat unid fusão (Econ energia) Lig/Desl]	R	R/W	R	R	R/W	R
[Timer semanal]	R	R/W	R	R	R/W	R
[Timer desl auto aquec de cola encad]	R	R/W	R	R	R/W	R

[Definições da interface]

[Rede]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Endereço IPv4 da máquina]*1	R	R	R/W	R	R/W	R
[Endereço do gateway IPv4]	R	R	R/W	R	R/W	R
[Endereço IPv6 da máquina]	R	R	R	R	R	R
[Endereço do gateway IPv6]	R	R	R	R	R	R
[Config aut de end s monitor. de estado IPv6]	R	R	R/W	R	R/W	R
[Configuração DHCPv6]	R	R	R/W	R	R/W	R
[Configuração de DNS]*2	R	R	R/W	R	R/W	R
[Configuração de DDNS]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R
[Nome de domínio]*1	R	R	R/W	R	R/W	R
[Configuração de WINS]	R	R	R/W	R	R/W	R
[Protocolo efetivo]	R	R	R/W	R	R/W	R
[Protocolo de entrega NCP]	R	R	R/W	R	R/W	R
[Tipo de quadro NW]	R	R	R/W	R	R/W	R
[Nome do computador de SMB]	R	R	R/W	R	R/W	R
[Grupo de trabalho de SMB]	R	R	R/W	R	R/W	R
[Velocidade de Ethernet]	R	R	R/W	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Comando ping]	–	–	R/W	–	R/W	R
[Permitir comunicação SNMPv3]	R	R	R/W	R	R/W	R
[Permitir comunicação SSL/TLS]	R	R	R/W	R	R/W	R
[Nome do host]	R	R	R/W	R	R/W	R
[Nome da máquina]	R	R	R/W	R	R/W	R
[Autenticação IEEE 802.1X para Ethernet]	R	R	R/W	R	R/W	R
[Restaurar autenticação IEEE 802.1X para padrões]	–	–	R/W	–	R/W	–

*1 Quando a opção Obter auto está definida, os dados são apenas de leitura.

*2 Todos os administradores e usuários podem executar testes de conexões.

[Imprimir lista]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Imprimir lista]	–	–	R/W	–	R/W	–

[Transferência de arquivos]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Servidor SMTP]	R	R	R/W	R	R/W	R
[Autenticação SMTP]*3	R	R/W	R	R	R/W	R
[POP antes de SMTP]	R	R/W	R	R	R/W	R
[Protocolo de recebimento]	R	R/W	R	R	R/W	R
[Definições de POP3/IMAP4]	R	R/W	R	R	R/W	R
[Endereço de e-mail do administrador]	R	R/W	R	R	R/W	R
[Porta de comunicação de e-mail]	R	R	R/W	R	R/W	R
[Intervalo de recebimento de e-mail]	R	R	R/W	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Tamanho máx. de recebimento de e-mail]	R	R	R/W	R	R/W	R
[Armazenam. de e-mail no servidor]	R	R	R/W	R	R/W	R
[Nome de usuário/senha padrão (Enviar)]*3	R	R/W	R	R	R/W	R
[Programar/Alterar/Excluir mensagem de e-mail]	R	R/W	R	R	R/W	R/W
[Especificar automat nome do remet]	R	R	R/W	R	R/W	R
[Temp intervalo de reenv do scanner]	R	R	R/W	R	R/W	R
[Número de reenvios do scanner]	R	R	R/W	R	R/W	R

*3 As senhas não podem ser lidas.

[Ferramentas administrador]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Gerenciamento de catálogo de endereços]	R/W	R/W *4	R/W *4	R/W *4	R/W *5	R*5
[Catálogo de endereços: Programar/ Alterar/Excluir grupo]	R/W	R/W *4	R/W *4	R/W *4	R/W *5	R*5
[Catálogo de endereços: Alterar ordem]	R/W	–	–	–	R/W	–
[Imprimir catálogo de endereços: Lista de destinos]	R/W	–	–	–	R/W	R/W
[Catálogo de endereços: Editar título]	R/W	–	–	–	R/W	–
[Catálogo de endereços: Trocar título]	R/W	–	–	–	R/W	R
[Fazer backup/Restaurar: Defs person usuár e Cat ender]	R/W	–	–	–	R/W	–
[Def de transp de dados p/ o programa aut do catál de end]	R/W	R	R	R	R/W	R
[Excluir aut usuário no Cat de end]	R/W	–	–	–	R/W	–

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Excluir todos os dados no Catálogo de endereços]	R/W	–	–	–	R/W	–
[Exibir/imprimir contador]	R	R/W	R	R	R/W	R/W
[Exibir/Zerar/Imprimir contador por usuário]	R/W*6	R/W*7	R	R	R/W	–
[Exibir/Apagar contador ecológico]	–	R/W	–	–	–	–
[Exibir/Apagar contador ecológico por usuário]	–	R/W	–	–	–	–
[Período do contador ecológico/Mensagem do administr]	R	R/W	R	R	R	R
[Ação da máq quando é ating o limite]	R	R/W	R	R	R	R
[Lim de uso de vol de impressão: Def de cont de unidade]	R	R/W	R	R	R	R
[Limite de uso de volume de impr avançado]	R	R/W	R	R	R	R
[Lim uso vol impressão: Valor limite padrão]	R/W	R	R	R	R	R
[Uso de slot para mídia]	R	R/W	R	R	R	R
[Gerenciamento de autenticação de usuário]	R	R/W	R	R	R/W	R
[Gerenciador de autenticação aprimorado]	R	R/W	R	R	R/W	R
[Gerenciamento de autenticação de administrador]	R/W *8*9	R/W *9	R/W *9	R/W *9	R/W	–
[Programar/Alterar administrador]	R/W*10	R/W*10	R/W*10	R/W*10	–	–
[Gerenciamento do contador de chave]	R	R/W	R	R	R/W	R
[Gerenciamento da unidade externa de carga]	R	R/W	R	R	R/W	R
[Gerenciamento da unidade externa de carga aprimorada]	R	R/W	R	R	R/W	R
[Segurança estendida]						

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
• [Chave de criptografia de driver]	–	–	R/W	–	R/W	–
• [Chave criptografia do driver: Nível cript]	R	R	R/W	R	R/W	R
• [Restringir visualiz de destinos de usuários]	R	R/W	R	R	R/W	R
• [Criptogr Defs personaliz do usuár e Cat endereços]	R/W	R	R	R	R	R
• [Aprimorar proteção de arquivo]	R	R	R	R/W	R	R
• [Restringir uso de destinos]	R/W	R	R	R	R	R
• [Restringir adição de destinos de usuários]	R/W	R	R	R	R	R
• [Definições por SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Autenticar tarefa atual]	R	R/W	R	R	R/W	R
• [Política de senha]	R/W	–	–	–	–	–
• [Serviço @Remote]	R	R/W	R	R	R/W	R
• [Atualizar firmware]	R	R/W	R	R	–	–
• [Alterar estrutura de firmware]	R	R/W	R	R	–	–
• [Violação de entrada de senha]	–	R/W	–	–	–	–
• [Definição de segurança para violação de acesso]	–	R/W	–	–	–	–
• [Violação de acesso ao dispositivo]	–	R/W	–	–	–	–
[Excluir arq aut no servidor de doc]	R	R	R	R/W	R/W	R
[Excluir todos os arquivos do servidor de documentos]	–	–	–	R/W	R/W	–
[Programar/Alterar/Excluir servidor LDAP] *3	–	R/W	–	–	R/W	R
[Pesquisa LDAP]	R	R/W	R	R	R/W	R

9

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Entrar no modo susp pelo timer do modo susp]	R	R/W	R	R	R/W	R
[Chamada de teste de serviço]	–	R/W	–	–	R/W	–
[Notificar status da máquina]	–	R/W	–	–	R/W	–
[Bloqueio do modo de serviço]	R	R/W	R	R	R/W	R
[Versão de firmware]	R	R	R	R	R	R
[Nível de segurança da rede]	R	R	R/W	R	R	R
[Definição p/ apagar automat a memo]	R	R/W	R	R	R	R
[Apagar toda a memória]	–	R/W	–	–	–	–
[Excluir todos os logs]	–	R/W	–	–	R/W	–
[Definição do log de transferência]*11	R	R/W	R	R	R/W	R
[Impr c/prev contra cópia não autor: Impressora]	R	R/W	R	R	R/W	R
[Programar/Alterar/Excluir região]	–	R/W	–	–	R/W	R
[Definições de criptografia de dados da máquina]	–	R/W	–	–	–	–
[Programar/Excluir certificado de dispositivo]	–	–	R/W	–	–	–
[Inf de definição do dispositivo: Def de import(servidor)]*12	–	–	–	–	–	–
[Informações de definição do dispositivo: Executar importação (Servidor)]*12	–	–	–	–	–	–
[Inf de definição do dispositivo: Export (disp arm mem)]*12	–	–	–	–	–	–
[Inf de definição do dispositivo: Import (disp arm mem)]*12	–	–	–	–	–	–
[Tipo de arquivo PDF: PDF/A fixo]	R	R/W	R	R	R/W	R
[Tecla Parar p/susp trabalho de impr]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Tecla de econ energia p/Alterar modo]	R	R/W	R	R	R/W	R
[Carimbo de segurança obrig: Copiadora]	R	R/W	R	R	R/W	R
[Carimbo de segurança obrig: Serv doc.]	R	R/W	R	R	R/W	R
[Carimbo de segurança obrig: Impress]	R	R/W	R	R	R/W	R
[User's Own Customization] (Personalização do usuário)	R	R/W	R	R	R/W	R
[Contador uso vol: Redefs programadas/ especificadas]	R	R/W	R	R	R	R
[Selecione as opções de idioma]	–	R/W	–	–	R/W	–
[Coletar logs]	R	R/W	R	R	R/W	R
[Gerenciamento central do Catálogo de endereços]						
• [Gerenciamento central do Catálogo de endereços]	R	R/W	R	R	R	R
• [Sincronização de clientes]*13	R/W	R/W	R	R	R	R
• [Sincronizar com servidor]*14	R/W	R/W	R	R	R	R

*3 As senhas não podem ser lidas.

*4 É possível alterar apenas cabeçalhos e pesquisas de usuários.

*5 Itens que podem ser executados, alterados e lidos variam de acordo com os privilégios de acesso.

*6 Pode ser apenas limpo.

*7 Pode ser apenas impresso.

*8 Essa definição não pode ser alterada quando a função de autenticação individual é usada.

*9 Apenas as definições de privilégios de administrador podem ser alteradas.

*10 Os administradores podem apenas alterar suas próprias contas.

*11 Pode ser alterado apenas para [Desligado].

*12 O administrador com todos os privilégios, incluindo privilégios de administrador de usuários, administrador do equipamento, administrador da rede e administrador de arquivos, pode executar R/W (Leitura/Gravação).

*13 Aparece quando você usa o equipamento como servidor.

*14 Aparece quando você usa o equipamento como cliente.

Definições da bandeja de papel

Esta seção relaciona as definições exibidas ao pressionar a tecla [Definição de papel] no painel de controle.

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo das configurações em "Definições disponíveis".

[Defin do papel da band]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Bandeja de papel]	R	R/W	R	R	R/W	R
[Tampa/Designação/Separador/Folha de separação]	R	R/W	R	R	R/W	R
[Editar papel personalizado]	–	R/W	–	–	R/W	–

Editar página principal

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo das configurações em "Definições disponíveis".

[Editar tela inicial]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Mover ícone]	R	R/W	R	R	R/W	R
[Excluir ícone]	R	R/W	R	R	R/W	R
[Adicionar ícone]	–	R/W	–	–	R/W	–
[Restaurar exibição padrão ícones]	–	R/W	–	–	R/W	–
[Inserir imagem na tela inicial]	–	R/W	–	–	R/W	–

Definições de ajuste para operadores.

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definições de ajuste para operadores]	R/W	R/W	R/W	R/W	R/W	R/W

Definições de ajuste para operadores qualificados

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definições de ajuste para operadores qualificados]	–	R/W	–	–	–	–

Recursos do servidor de copiadora/documentos

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

[Caract gerais]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Prioridade da dens autom de imagem]	R	R/W	R	R	R	R
[Prioridade do tipo original]	R	R/W	R	R	R	R
[Prioridade do tipo de foto original]	R	R/W	R	R	R	R
[Orientação original no modo duplex]	R	R/W	R	R	R	R
[Orientação de cópia no modo duplex]	R	R/W	R	R	R	R
[Modo de reserva de trabalho]	R	R/W	R	R	R	R
[Timer desl aut da tela reserva]	R	R/W	R	R	R	R
[Quantidade máx. de cópias]	R	R/W	R	R	R	R
[Redef manual do contador de orig]	R	R/W	R	R	R	R
[Troca automática de bandeja]	R	R/W	R	R	R	R
[Fundo escuro]	R	R/W	R	R	R	R
[Padrão de recursos do painel]	R	R/W	R	R	R	R
[Prioridade de ajuste de imagem]	R	R/W	R	R	R	R
[Monitor de papel]	R	R/W	R	R	R	R
[Exibição do tipo do original]	R	R/W	R	R	R	R
[Alerta Sonoro: Orig deixado no vidro de expos]	R	R/W	R	R	R	R
[Chamada de fim de trabalho]	R	R/W	R	R	R	R
[Trocar monitor de contador de origin]	R	R/W	R	R	R	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Tela de definições de papel p/band A]	R	R/W	R	R	R	R
[Personalizar função: Copiadora]	R	R/W	R	R	R/W	R
[Personal função: Armazen do servidor de doc]	R	R/W	R	R	R/W	R

[Taxa de reprodução]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Reduzir/Ampliar atalho]	R	R/W	R	R	R	R
[Taxa de reprodução]	R	R/W	R	R	R	R
[Prioridade de taxa redução/ampliação]	R	R/W	R	R	R	R
[Taxa para criar margem]	R	R/W	R	R	R	R

[Editar]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Margem da frente: Esquerda/direita]	R	R/W	R	R	R	R
[Margem do verso: Esquerda/direita]	R	R/W	R	R	R	R
[Margem da frente: Para cima/baixo]	R	R/W	R	R	R	R
[Margem do verso: Para cima/baixo]	R	R/W	R	R	R	R
[1l→Margem aut de 2l: cima/cima]	R	R/W	R	R	R	R
[1l→Margem aut de 2l: cima/bxo]	R	R/W	R	R	R	R
[Definição de encolhim para revista]	R	R/W	R	R	R	R
[Apagar a largura da borda]	R	R/W	R	R	R	R
[Apagar sombra do original ao combin]	R	R/W	R	R	R/W	R
[Apagar largura central]	R	R/W	R	R	R	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Cópia da capa ao combinar]	R	R/W	R	R	R/W	R
[Ordem de cópia ao combinar]	R	R/W	R	R	R/W	R
[Orientação: Folheto, revista]	R	R/W	R	R	R/W	R
[Linha de separação de repet de img]	R	R/W	R	R	R/W	R
[Linha de separação de cópias duplas]	R	R/W	R	R	R/W	R
[Linha de separação ao combinar]	R	R/W	R	R	R/W	R
[Cópia da pág de designação ao combin]	R	R/W	R	R	R/W	R
[Copiar a contracapa]	R	R/W	R	R	R/W	R
[Posição de cópias duplas]	R	R/W	R	R	R/W	R

[Carimbo]

[Carimbo predef]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Idioma do carimbo]	R	R/W	R	R	R/W	R
[Prioridade do carimbo]	R	R/W	R	R	R	R
[Formato do carimbo]: COPY	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: URGENTE	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: PRIORIDADE	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: Para sua informação.	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: PRELIMINAR	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: Apenas para uso interno	R	R/W	R	R	R/W*1	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Formato do carimbo]: CONFIDENCIAL	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: RASCUNHO	R	R/W	R	R	R/W*1	R
[Formato do carimbo]: CÓPIA	R	R/W	R	R	R	R
[Formato do carimbo]: URGENTE	R	R/W	R	R	R	R
[Formato do carimbo]: PRIORIDADE	R	R/W	R	R	R	R
[Cor do carimbo]: Para sua informação.	R	R/W	R	R	R	R
[Cor do carimbo]: PRELIMINAR	R	R/W	R	R	R	R
[Cor do carimbo]: Apenas para uso interno	R	R/W	R	R	R	R
[Cor do carimbo]: CONFIDENCIAL	R	R/W	R	R	R	R
[Cor do carimbo]: Rascunho	R	R/W	R	R	R	R

*1 Apenas ajustes da posição de impressão podem ser especificados. A posição de impressão não pode ser configurada.

[Carimbo usuário]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Programar/excluir carimbo]	R	R/W	R	R	R/W	R
[Formato do carimbo]: 1-5	R	R/W	R	R	R/W	R
[Cor do carimbo]: 1-5	R	R/W	R	R	R/W	R

[Carimbo de data]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Formato]	R	R/W	R	R	R	R
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Sobrepor]	R	R/W	R	R	R/W	R
[Cor do carimbo]	R	R/W	R	R	R	R
[Definição de carimbo]	R	R/W	R	R	R/W*2	R

*2 Apenas ajustes da posição de impressão podem ser definidos. A posição de impressão não pode ser configurada.

[Numeração página]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Formato do carimbo]	R	R/W	R	R	R	R
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R
[Posição de carimbo pág tras de duplex]	R	R/W	R	R	R/W	R
[Numeração de página ao combinar]	R	R/W	R	R	R/W	R
[Estampar no separador de designação]	R	R/W	R	R	R/W	R
[Posição do carimbo:P1,P2...]	R	R/W	R	R	R/W*3	R
[Posição do carimbo:1/5,2/5...]	R	R/W	R	R	R/W*3	R
[Posição do carimbo:-1-,-2-...]	R	R/W	R	R	R/W*3	R
[Posição do carimbo:P.1,P.2...]	R	R/W	R	R	R/W*3	R
[Posição do carimbo:1,2...]	R	R/W	R	R	R/W*3	R
[Posição do carimbo:1-1,1-2...]	R	R/W	R	R	R/W*3	R
[Sobrepor]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Cor do carimbo]	R	R/W	R	R	R	R
[Letra inicial da numeração de página]	R	R/W	R	R	R	R

*3 Apenas ajustes da posição de impressão podem ser definidos. A posição de impressão não pode ser configurada.

[Texto do carimbo]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Fonte]	R	R/W	R	R	R/W	R
[Tamanho]	R	R/W	R	R	R/W	R
[Sobrepor]	R	R/W	R	R	R/W	R
[Cor do carimbo]	R	R/W	R	R	R	R
[Definição de carimbo]	R	R/W	R	R	R/W	R
[Alterar nº de série do trab p/ 1º trab]	R	R/W	R	R	R	R

[Entrada/Saída]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Redefinição automática de SADF]	R	R/W	R	R	R	R
[Cop método face de ejeção no modo de vidro]	R	R/W	R	R	R	R
[Reinic leitura aut de mem integral]	R	R/W	R	R	R	R
[Def classif/empil band de separ em espinha]	R	R/W	R	R	R	R
[Inserir folha de separação]	R	R/W	R	R	R	R
[Definição de papel timbrado]	R	R/W	R	R	R	R
[Definição de corte da borda frontal]	R	R/W	R	R	R	R
[Posição de grampeamento]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Tipo de perfuração]	R	R/W	R	R	R/W	R
[Encadernação de argolas / Tipo de dobra / Band saída do empil]*4	R	R/W	R	R	R/W	R
[Finalizador: Posição de grampeamento]	R	R/W	R	R	R/W	R
[Finalizador: Tipo de perfuração]	R	R/W	R	R	R/W	R
[Finalizador: Tipo de encadernação de argolas]	R	R/W	R	R	R/W	R
[Tela simplificada: Tipos de acabamento]	R	R/W	R	R	R/W	R
[Defs dobra simples(Finalizador:Band de folheto]	R	R/W	R	R	R	R
[Bandeja de saída da dobra em Z]	R	R/W	R	R	R	R
[Definições de dobra simples]	R	R/W	R	R	R	R
[Definições de dobra de carta p/ fora]	R	R/W	R	R	R	R
[Definições dobra de carta p/dentro]	R	R/W	R	R	R	R
[Definições de dobra dupla paralela]	R	R/W	R	R	R	R
[Definições de dobra em portada]	R	R/W	R	R	R	R

*4 Os nomes dos itens variam de acordo com os opcionais instalados.

[Ajustar imagem color]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Densidade de fundo para ADS (Cor integral/duas cores)]	R	R/W	R	R	R/W	R
[Sensibilidade de cor]	R	R/W	R	R	R/W	R
[Sensibilidade A.C.S.]	R	R/W	R	R	R/W	R
[Prioridade A.C.S.]	R	R/W	R	R	R/W	R

[Ferramentas administrador]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Proteger menu]	R	R/W	R	R	R	R

Funções da Impressora

Esta seção lista as funções da impressora que aparecem se [Impressora] na Tela inicial for pressionado.

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

Funções da Impressora

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Lista trabalhos]	R	R	R	R	R	R
[Trabs impr]	R	R	R	R/W	R/W	R/W
[Imp a partir do disp de armaz de mem]	–	–	–	–	R/W	R/W
[Redefinir trab]	R/W	R/W	R/W	R/W	R/W	R/W
[Operação trab]	R/W	R/W	R/W	R/W	R/W	R/W
[AlimForm]	R/W	R/W	R/W	R/W	R/W	R/W
[Lista trabs em spool]	R	R/W	R	R	R	R
[Log de erros]	–	R	–	–	R	R

Características da impressora

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

[Listar/Testar impressão]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Listas múltiplas]	–	R/W	–	–	R/W	R/W
[Página de configuração]	–	R/W	–	–	R/W	R/W
[Log de erros]	–	R/W	–	–	R/W	R/W
[Página de configuração/fontes de PCL]	–	R/W	–	–	R/W	R/W
[Página de configuração/fontes de PS]	–	R/W	–	–	R/W	R/W
[Página de configuração/fontes de PDF]	–	R/W	–	–	R/W	R/W
[Despejo hexadecimal]	–	R/W	–	–	R/W	R/W

[Gerenciamento de dados]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Proteger menu]	R	R/W	R	R	R	R
[Listar/Testar bloqueio de impressão]	R	R/W	R	R	R	R
[Excluir todos os trab imp temporár]	–	–	–	R/W	–	–
[Excluir todos os trab de imp armaz]	–	–	–	R/W	–	–
[Excluir autom os trab de imp temp]	R	R	R	R/W	R	R
[Excluir autom os trab de imp armaz]	R	R	R	R/W	R	R
[Modo gráfico em quatro cores]	R	R	R	R/W	R	R

[Sistema]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Relatório de erro de impressão]	R	R/W	R	R	R	R
[Continuar automaticamente]	R	R/W	R	R	R	R
[Armazenar e ignorar trabalho c/erro]	R	R/W	R	R	R	R
[Estouro de memória]	R	R/W	R	R	R	R
[Canc aut confirm trab c/erro PDL]	R	R/W	R	R	R	R
[Canc aut p/ trab(s) de impr c/erro]	R	R/W	R	R	R	R
[Separação de trabalhos]	R	R/W	R	R	R	R
[Girar 180 graus]	R	R/W	R	R	R	R
[Imprimir dados compactados]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Cópias]	R	R/W	R	R	R	R
[Impressão de página em branco]	R	R/W	R	R	R	R
[Imagem em spool]	R	R/W	R	R	R	R
[Tempo de espera do trab reservado]	R	R/W	R	R	R	R
[Idioma da impressora]	R	R/W	R	R	R	R
[Tamanho de papel secundário]	R	R/W	R	R	R	R
[Tamanho da página]	R/W	R/W	R	R	R	R
[Definição de papel timbrado]	R	R/W	R	R	R	R
[Prioridade de definição de bandeja]	R	R/W	R	R	R	R
[Impressão de borda a borda]	R	R/W	R	R	R	R
[Idioma padrão da impressora]	R	R/W	R	R	R	R
[Troca de bandeja]	R	R/W	R	R	R	R
[Troca automát avançada de bandeja]	R	R/W	R	R	R	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Trabs não impressos, pois máq desl]	R	R/W	R	R	R	R
[Restringir trabs de impressão direta]	R	R/W	R	R	R	R
[Trocar tela inicial]	R	R/W	R	R	R	R

[Interface do host]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Buffer de E/S]	R	R/W	R	R	R	R
[Tempo limite de E/S]	R	R/W	R	R	R	R

[Menu PCL]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Orientação]	R	R/W	R	R	R	R
[Linhas do formulário]	R	R/W	R	R	R	R
[Origem da fonte]	R	R/W	R	R	R	R
[Número de fonte]	R	R/W	R	R	R	R
[Tamanho do ponto]	R	R/W	R	R	R	R
[Densidade da fonte]	R	R/W	R	R	R	R
[Conjunto de símbolos]	R	R/W	R	R	R	R
[Fonte Courier]	R	R/W	R	R	R	R
[Largura A4 estendida]	R	R/W	R	R	R	R
[Anexar CR a LF]	R	R/W	R	R	R	R
[Resolução]	R	R/W	R	R	R	R

[Menu PS]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Tempo limite de trabalho]	R	R/W	R	R	R	R
[Tempo limite de espera]	R	R/W	R	R	R	R
[Método de seleção de papel]	R	R/W	R	R	R	R
[Altern entre funções de impr 1/2 lds]	R	R/W	R	R	R	R
[Formato de dados]	R	R/W	R	R	R	R
[Resolução]	R	R/W	R	R	R	R
[Economia de toner]	R	R/W	R	R	R	R
[Definição de cor]	R	R/W	R	R	R	R
[Perfil de cores]	R	R/W	R	R	R	R
[Modelo de cores de processo]	R	R/W	R	R	R	R
[Detecção automática de orientação]	R	R/W	R	R	R	R
[Reprodução de cinza]	R	R/W	R	R	R	R

[Menu PDF]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Alterar senha de PDF]	R	R/W	R	R	R	R
[Senha de grupo do PDF]	R	R/W	R	R	R	R
[Impressão em ordem inversa]	R	R/W	R	R	R	R
[Resolução]	R	R/W	R	R	R	R
[Economia de toner]	R	R/W	R	R	R	R
[Definição de cor]	R	R/W	R	R	R	R
[Perfil de cores]	R	R/W	R	R	R	R
[Modelo de cores de processo]	R	R/W	R	R	R	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Detecção automática de orientação]	R	R/W	R	R	R	R

Recursos de scanner

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

[Definições gerais]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Trocar título]	R	R/W	R	R	R	R
[Pesquisar destino]	R	R/W	R	R	R	R
[Aut ext: Def substituição caminho da pasta]	R	R/W	R	R	R	R
[Tempo esp do com de varred do PC]	R	R/W	R	R	R	R
[Prior de exib da lista de destino 1]	R	R/W	R	R	R	R
[Prior exibição da lista de destino 2]	R	R/W	R	R	R	R
[Imprimir e excluir o diário do scanner]	R	R/W	R	R	R	R
[Imprimir diário do scanner]	R	R/W	R	R	R	R
[Excluir diário do scanner]	R	R/W	R	R	R	R
[Excluir destinos recentes]	R	R/W	R	R	R	R
[Usar WSD ou DSM]	R	R/W	R	R	R/W	R
[Usar uma lista de destinos que não seja DSM]	R	R/W	R	R	R/W	R
[Programar definição para destinos]	R	R/W	R	R	R	R

[Definições de leitura]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Nível de sensibilidade A.C.S.]	R	R/W	R	R	R	R
[Tempo espera pelo próx orig: Vidro de expo]	R	R/W	R	R	R	R

Definições	Usuár io	Equip	N/W	Arqui vo	Nív.1	Nív.2
[Tempo de espera pelo(s) próx(s) orig(is): SADF]	R	R/W	R	R	R	R
[Densidade de fundo para ADS (Cor integral)]	R	R/W	R	R	R	R
[Detectar página em branco]	R	R/W	R	R	R	R
[Taxa de reprodução]	R	R/W	R	R	R	R
[Program/Alter/Excl tamanho leitura]	R	R/W	R	R	R	R

[Definições de envio]

Definições	Usuár io	Equip	N/W	Arqui vo	Nív.1	Nív.2
[Compactação(Preto e branco)]	R	R/W	R	R	R/W	R
[Método compact (preto e branco)]	R	R/W	R	R	R/W	R
[Compactação (Escala de cinza/Cor integral)]	R	R/W	R	R	R/W	R
[Mét de compact para PDF de alta compactação]	R	R/W	R	R	R/W	R
[Nível de PDF de alta compactação]	R	R/W	R	R	R/W	R
[PDF digitalizado c/OCR: Sensib págs em branco]	R	R/W	R	R	R/W	R
[Tamanho máx. de e-mail]	R	R	R/W	R	R	R
[Dividir e enviar e-mail]	R	R	R/W	R	R	R
[Inserir inform adicionais de e-mail]	R	R/W	R	R	R/W	R
[N° de dígitos p/ arq de páginas únicas]	R	R/W	R	R	R/W	R
[Método de e-mail em arquivo armazen]	R	R/W	R	R	R/W	R
[Assunto padrão de e-mail]	R	R/W	R	R	R	R

[Definições iniciais]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Proteger menu]	R	R/W	R	R	R	R

Definições de recurso estendido

[Definições de recurso estendido]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definição de inicialização]	R	R/W	R	R	R	R
[Instalar]	R	R/W	R	R	R	R
[Desinstalar]	R	R/W	R	R	R	R
[Informações sobre recurso estendido]	R	R/W	R	R	R	R
[Ferramentas administrador]	–	R/W	–	–	–	–
[Defin de inicial de progr adicional]	R	R/W	R	R	R	R
[Instalar progr adicional]	R	R/W	R	R	R	R
[Desinstalar progr adicional]	R	R/W	R	R	R	R
[Informações progr adicional]	R	R/W	R	R	R	R

Manutenção

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

[Manutenção]

Definições	Usuár io	Equip	N/W	Arqui vo	Unset	Defini do
[Calibragem automática de cor]	–	R/W	–	–	R/W	–
[Registro de cor]	–	R/W	–	–	R/W	–

9

Web Image Monitor: Exibir contador ecológico

Estas definições estão em [Estado/informações].

Um usuário pode ver apenas o seu próprio contador.

Definições	Usuári o	Equip	N/W	Arqui vo	Unset	Defini do
[Download]	–	R/W	–	–	–	–
[Contador total do dispositivo]	–	R	–	–	–	–
[Contador por usuário]	–	R	–	–	R	R

Web Image Monitor: Trabalho

Estas definições estão em [Estado/informações].

Os usuários só podem alterar trabalhos que eles mesmos executaram.

[Lista de trabalhos]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Trabalhos atuais/em espera]: [Excluir reserva]	–	R/W	–	–	–	R/W
[Trabalhos atuais/em espera]: [Suspender impressão]/[Continuar impressão]	–	R/W	–	–	–	–
[Trabalhos atuais/em espera]: [Alterar ordem]	–	R/W	–	–	–	–
[Histórico de trabalhos]	–	R	–	–	R	R[*1]

*1 Pode ser exibido quando a autenticação do código de usuário esteja ativada para o método de autenticação do usuário.

[Impressora]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Impressão em spool]: [Excluir]	R	R/W	R	R	R	R
[Histórico de trabalhos]	R	R/W	R	R	R	R
[Log de erros]	–	R	–	–	R	R

[Servidor de documentos]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Histórico de trabalhos de impressão]	–	R	–	–	R	R[*1]
[Histórico de envio remoto do scanner]	–	R	–	–	R	R[*1]

*1 Pode ser exibido quando a autenticação do código de usuário esteja ativada para o método de autenticação do usuário.

Web Image Monitor: Definições de dispositivo

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

[Sistema]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Nome do dispositivo]	R	R	R/W	R	R/W	R
[Comentário]	R	R	R/W	R	R/W	R
[Local]	R	R	R/W	R	R/W	R
[Idioma do painel]	R	R/W	R	R	R/W	R
[Impressão em spool]	R	R/W	R	R	R/W	R
[Proteger painel da impressora]	R	R/W	R	R	–	–
[Prioridade de impressão]	R	R/W	R	R	R/W	R
[Timer de redefinição de função]	R	R/W	R	R	R/W	R
[Tecla de economia de energia para alterar modo]	R	R/W	R	R	R/W	R
[Tecla Parar para suspender trabalho de impressão]	R	R/W	R	R	R/W	R
[Exibir endereço IP no painel do dispositivo]	R	R/W	R	R	–	–
[Uso de slot para mídia]	R	R/W	R	R	R	R
[ID compatível]	R	R/W	R	R	R/W	R
[Tipo de arquivo PDF: PDF/A fixo]	R	R/W	R	R	R/W	R
[Proibir a impressão de arquivos armazenados do Web Image Monitor]	R	R/W	R	R	R	R
[Bandeja de saída]	R	R/W	R	R	R/W	R
[Prioridade de Bandeja de papel]	R	R/W	R	R	R/W	R
[Bandeja da folha de capa]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Bandeja da folha de contracapa]	R	R/W	R	R	R/W	R
[Bandeja de separadores]	R	R/W	R	R	R/W	R
[Bandeja de folha de designação 1-11]	R	R/W	R	R	R/W	R
[Bandeja de folha de separação]	R	R/W	R	R	R/W	R

[Alocação da tecla de função/Prioridade da função]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Alocação da tecla de função]	R	R/W	R	R	R/W	R
[Prioridade da função]	R	R/W	R	R	R/W	R

[Papel]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Bandeja 1-8]	R	R/W	R	R	R/W	R
[Bandeja A]	R	R/W	R	R	R/W	R
[Bandeja superior do intermediário]	R	R/W	R	R	R/W	R
[Bandeja inferior do intermediário]	R	R/W	R	R	R/W	R
[Bandeja superior do intermediário de encadernação sem costura]	R	R/W	R	R	R/W	R
[Bandeja inferior do intermediário da encadernadora]	R	R/W	R	R	R/W	R
[Detecção de pouco papel]	R	R/W	R	R	R	R

[Papel personalizado]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Programar/Alterar]	–	R/W	–	–	R/W	–

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Excluir]	–	R/W	–	–	R/W	–
[Lembrar biblioteca de papel]	–	R/W	–	–	R/W	–

[Data/Hora]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definir data]	R	R/W	R	R	R/W	R
[Definir hora]	R	R/W	R	R	R/W	R
[Nome do servidor SNTP]	R	R/W	R	R	R/W	R
[Intervalo de polling de SNTP]	R	R/W	R	R	R/W	R
[Fuso horário]	R	R/W	R	R	R/W	R

[Timer]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Timer do modo de suspensão]	R	R/W	R	R	R/W	R
[Timer do modo de baixa energia]	R	R/W	R	R	R/W	R
[Timer de redefinição automática do sistema]	R	R/W	R	R	R/W	R
[Timer de redefinição automática da copiadora/servidor de documentos]	R	R/W	R	R	R/W	R
[Timer de redefinição automática do scanner]	R	R/W	R	R	R/W	R
[Timer de redefinição automática da impressora]	R	R/W	R	R	R/W	R
[Timer de logout automático]	R	R/W	R	R	R/W	R
[Modo de desativação da unidade de fusão Lig/Dsl]	R	R/W	R	R	R/W	R
[Timer semanal]	R	R/W	R	R	R/W	R

[Logs]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Log de trabalhos]	R	R/W	R	R	R/W	R
[Log de acessos]	R	R/W	R	R	R/W	R
[Logs ecológicos]	R	R/W	R	R	R/W	R
[Transferir logs]*2	R	R/W	R	R	R/W	R
[Código de classificação]	R	R/W	R	R	R/W	R
[Excluir todos os logs]	–	R/W	–	–	R/W	–

*2 Pode ser alterado apenas para [Inativo].

[Fazer download de logs]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Logs para download]	–	R/W	–	–	–	–
[Download]	–	R/W	–	–	–	–

[E-mail]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Endereço de e-mail do administrador]	–	R/W	–	–	R/W	R
[Especificar automat nome do remet]	–	R/W	–	–	R/W	R
[Assinatura]	–	R/W	–	–	R/W	R
[Protocolo de recebimento]	–	R/W	–	–	R/W	R
[Intervalo de recebimento de e-mail]	–	–	R/W	–	R/W	R
[Tamanho máx. de recebimento de e-mail]	–	–	R/W	–	R/W	R
[Armazenamento de e-mail no servidor]	–	–	R/W	–	R/W	R
[Nome do servidor SMTP]	–	–	R/W	–	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Nº da porta SMTP]	–	–	R/W	–	R/W	R
[Usar conexão segura (SSL)]	–	–	R/W	–	R/W	R
[Autenticação SMTP]	–	R/W	–	–	R/W	R
[Endereço de e-mail de aut. SMTP]	–	R/W	–	–	R/W	R
[Nome do usuário de aut. SMTP]	–	R/W	–	–	R/W	–
[Senha de aut. SMTP]*3	–	R/W	–	–	R/W	–
[Criptografia de aut. SMTP]	–	R/W	–	–	R/W	R
[POP antes de SMTP]	–	R/W	–	–	R/W	R
[Endereço de e-mail POP]	–	R/W	–	–	R/W	R
[Nome de usuário POP]	–	R/W	–	–	R/W	–
[Senha POP]*3	–	R/W	–	–	R/W	–
[Definição de tempo limite após aut. POP]	–	R/W	–	–	R/W	R
[Nome do servidor POP3/IMAP4]	–	R/W	–	–	R/W	R
[Criptografia POP3/IMAP4]	–	R/W	–	–	R/W	R
[Nº da porta de recebimento POP3]	–	–	R/W	–	R/W	R
[Nº da porta de recebimento IMAP4]	–	–	R/W	–	R/W	R
[Endereço de e-mail de notificação de e-mail]	–	R/W	–	–	R/W	R
[Receber notificação de e-mail]	–	R/W	–	–	R/W	–
[Nome de usuário de notificação de e-mail]	–	R/W	–	–	R/W	–
[Senha de notificação de e-mail]*3	–	R/W	–	–	R/W	–

*3 As senhas não podem ser lidas.

9

[Notificação de e-mail automática]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Mensagem de notificação]	R	R/W	R	R	R/W	R
[Grupos a notificar]	R	R/W	R	R	R/W	R
[Selecionar grupos/itens a serem notificados]	R	R/W	R	R	R/W	R
[Definições detalhadas de cada item]	R	R/W	R	R	R/W	R

[Notificação de e-mail sob demanda]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Assunto da notificação]	R	R/W	R	R	R/W	R
[Mensagem de notificação]	R	R/W	R	R	R/W	R
[Restrição de acesso às informações]	R	R/W	R	R	R/W	R
[Definições de endereço de e-mail/nome de domínio que pode ser recebido]	R	R/W	R	R	R/W	R

[Transferência de arquivos]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Nome de usuário de SMB]	–	R/W	–	–	R/W	–
[Senha de SMB]*3	–	R/W	–	–	R/W	–
[Nome de usuário de FTP]	–	R/W	–	–	R/W	–
[Senha de FTP]*3	–	R/W	–	–	R/W	–
[Nome de usuário de NCP]	–	R/W	–	–	R/W	–
[Senha de NCP]*3	–	R/W	–	–	R/W	–

*3 As senhas não podem ser lidas.

[Gerenciamento de autenticação de usuário]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Gerenciamento de autenticação de usuário]	R	R/W	R	R	R/W	R
[Definições de autenticação de trabalho da impressora]	R	R/W	R	R	R/W	R
[Definições de autenticação de código de usuário]	R	R/W	R	R	R/W	R
[Definições de autenticação básica]	R	R/W	R	R	R/W	R
[Definições de autenticação do Windows]	R	R/W	R	R	R/W	R
[Definições de grupo para autenticação do Windows]	R	R/W	R	R	R/W	R
[Definições de autenticação de LDAP]	R	R/W	R	R	R/W	R

[Gerenciamento de autenticação de administrador]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Autenticação do administrador de usuário]	R/W	R	R	R	R	R
[Autenticação do administrador de máquina]	R	R/W	R	R	R	R
[Autenticação do administrador de rede]	R	R	R/W	R	R	R
[Autenticação do administrador de arquivo]	R	R	R	R/W	R	R

[Programar/Alterar administrador]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Administrador de usuário]	R/W	R	R	R	–	–
[Administrador da máquina]	R	R/W	R	R	–	–
[Administrador de rede]	R	R	R/W	R	–	–
[Administrador de arquivo]	R	R	R	R/W	–	–

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Nome de usuário de login]*4	R/W	R/W	R/W	R/W	–	–
[Senha de login]*4	R/W	R/W	R/W	R/W	–	–
[Senha de criptografia]*4	R/W	R/W	R/W	R/W	–	–

*4 Os administradores podem apenas alterar suas próprias contas.

[Limitação de uso de volume de impressão]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Ação da máquina quando é atingido o limite]	R	R/W	R	R	R	R
[Limitação de uso de volume de impressão: Definição de contagem de unidade]	R	R/W	R	R	R	R
[Contador de uso de volume: Definições de redefinição programada/especificada]	R	R/W	R	R	R	R

[Servidor LDAP]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Pesquisa LDAP]	–	R/W	–	–	R/W	–
[Alterar]	–	R/W	–	–	R/W	–
[Excluir]	–	R/W	–	–	R/W	–

[Atualização de firmware]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Atualizar]	–	R/W	–	–	–	–
[Versão do firmware]	–	R	–	–	–	–

[Autenticação Kerberos]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Algoritmo de criptografia]	–	R/W	–	–	–	–
[Região 1-5]	–	R/W	–	–	–	–

[Informações de definição do dispositivo: Definição de importação (servidor)]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Importar arquivo de]*5	–	–	–	–	–	–
[Importação programada na Hora especificada]*5	–	–	–	–	–	–
[Comparando novo arquivo com o último arquivo importado]*5	–	–	–	–	–	–
[Notificação de falhas de e-mail]*5	–	–	–	–	–	–
[Número de novas tentativas]*5	–	–	–	–	–	–
[Intervalo para nova tentativa]*5	–	–	–	–	–	–
[Chave de criptografia]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, incluindo os privilégios de administrador de usuários, administrador do equipamento, administrador da rede e administrador de arquivos.

[Teste de importação]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Iniciar]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, incluindo os privilégios de administrador de usuários, administrador do equipamento, administrador da rede e administrador de arquivos.

[Importar/Exportar informações de definição do dispositivo]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Exportar informações de definição do dispositivo]*5	–	–	–	–	–	–
[Importar informações de definição do dispositivo]*5	–	–	–	–	–	–
[Exportar arquivo de imagem para tela inicial]*5	–	–	–	–	–	–

*5 R/W é o administrador com todos os privilégios, incluindo os privilégios de administrador de usuários, administrador do equipamento, administrador da rede e administrador de arquivos.

[Período do contador ecológico/Mensagem do administrador]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Exibir tela de informações]	R	R/W	R	R	R/W	R
[Exibir hora]	R	R/W	R	R	R/W	R
[Período de contagem]	R	R/W	R	R	R/W	R
[Período de contagem (dias)]	R	R/W	R	R	R/W	R
[Mensagem do administrador]	R	R/W	R	R	R/W	R

[Carimbo de segurança obrigatório]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Copiadora]	R	R/W	R	R	R	R
[Servidor de documentos]	R	R/W	R	R	R	R
[Impressora]	R	R/W	R	R	R	R

[Prevenção contra cópia não autorizada: Impressora]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definição de prevenção contra copia não autorizada]	R	R/W	R	R	R	R
[Prevenção contra cópia não autorizada obrigatória]	R	R/W	R	R	R	R
[Tipo de prevenção contra cópia não autorizada]	R	R/W	R	R	R	R
[Tipo de máscara para Padrão/Densidade/Efeito]	R	R/W	R	R	R	R
[Definições de texto de prevenção]	R	R/W	R	R	R	R

[Program/Change USB Device List]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Device 1]	R	R/W	R	R	R/W	R
[Device 2]	R	R/W	R	R	R/W	R

Web Image Monitor: Impressora

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

[Definições básicas]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Relatório de erro de impressão]	R	R/W	R	R	R	R
[Continuar automaticamente]	R	R/W	R	R	R	R
[Estouro de memória]	R	R/W	R	R	R	R
[Confirmação automática de cancelamento para trabalho com erro de PDL]	R	R/W	R	R	R	R
[Cancelamento automático para trabalho(s) de impressão com erro]	R	R/W	R	R	R	R
[Separação de trabalhos]	R	R/W	R	R	R	R
[Excluir automaticamente os trabalhos de impressão temporários]	R	R	R	R/W	R	R
[Excluir automaticamente os trabalhos de impressão armazenados]	R	R	R	R/W	R	R
[Trabalhos não impressos, pois a máquina estava desligada]	R	R/W	R	R	R	R
[Girar 180 graus]	R	R/W	R	R	R	R
[Imprimir dados compactados]	R	R/W	R/W	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Cópias]	R	R/W	R	R	R	R
[Impressão de página em branco]	R	R/W	R	R	R	R
[Imagem em spool]	R	R/W	R	R	R	R
[Tempo de espera do trabalho reservado]	R	R/W	R	R	R	R

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Idioma da impressora]	R	R/W	R	R	R	R
[Tamanho de papel secundário]	R	R/W	R	R	R	R
[Tamanho da página]	R	R/W	R	R	R/W	R
[Definição papel timbrado]	R	R/W	R	R	R	R
[Prioridade de definição de bandeja]	R	R/W	R	R	R	R
[Armazenar e ignorar trabalho com erro]	R	R/W	R	R	R	R
[Impressão de borda a borda]	R	R/W	R	R	R	R
[Idioma padrão da impressora]	R	R/W	R	R	R	R
[Troca de bandeja]	R	R/W	R	R	R	R
[Bloquear lista de impressões de teste]	R	R/W	R	R	R	R
[Troca automática avançada de bandeja]	R	R/W	R	R	R	R
[Impressora virtual]	R	R/W	R	R	R	R
[Restringir trabalhos de impressão direta]	R	R/W	R	R	R	R
[Definição de troca da tela inicial]	R	R/W	R	R	R	R
[Interface do host]	R	R/W	R	R	R	R
[Menu PCL]	R	R/W	R	R	R	R
[Menu PS]	R	R/W	R	R	R	R
[Menu PDF]	R	R/W	R	R	R	R

[Parâmetros de bandeja (PCL)]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Parâmetros de bandeja (PCL)]	–	R/W	–	–	–	–

[Parâmetros de bandeja (PS)]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Parâmetros de bandeja (PS)]	–	R/W	–	–	–	–

[Senha temporária do PDF]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Senha temporária do PDF]	–	–	–	–	R/W	R/W

[Senha de grupo do PDF]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Senha de grupo do PDF]	–	R/W	–	–	–	–

[Senha fixa do PDF]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Senha fixa do PDF]	–	R/W	–	–	–	–

[Definições de impressora virtual]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Nome da impressora virtual]	R	R/W	R	R	R	R
[Protocolo]	R	R/W	R	R	R	R
[Relatório de erro de impressão]	R	R/W	R	R	R	R
[Separação de trabalhos]	R	R/W	R	R	R	R
[Girar 180 graus]	R	R/W	R	R	R	R
[Duplex]	R	R/W	R	R	R	R
[Cópias]	R	R/W	R	R	R	R

Definições	Usuár io	Equip	N/W	Arqui vo	Nív.1	Nív.2
[Impressão de página em branco]	R	R/W	R	R	R	R
[Tamanho de papel secundário]	R	R/W	R	R	R	R
[Bandeja de entrada]	R	R/W	R	R	R/W	R/W
[Tamanho da página]	R	R/W	R	R	R/W	R
[Tipo de papel]	R	R/W	R	R	R/W	R/W
[Bandeja de saída]	R	R/W	R	R	R/W	R/W
[Definição papel timbrado]	R	R/W	R	R	R	R
[Impressão de borda a borda]	R	R/W	R	R	R	R
[Menu PCL]	R	R/W	R	R	R	R
[Menu PS]	R	R/W	R	R	R	R
[Menu PDF]	R	R/W	R	R	R	R
[Definições de RHPP]	R	R/W	R	R	R/W	R/W

[Permissões para Idioma da impressora operar o sistema de arquivos]

Definições	Usuár io	Equip	N/W	Arqui vo	Nív.1	Nív.2
[PJL]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: Scanner

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da definição "Proteção de menus".

[Definições gerais]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Trocar título]	R	R/W	R	R	R	R
[Pesquisar destino]	R	R/W	R	R	R	R
[Tempo de espera do comando de varredura do PC]	R	R/W	R	R	R	R
[Prioridade de exibição da lista de destino 1]	R	R/W	R	R	R	R
[Prioridade de exibição da lista de destino 2]	R	R/W	R	R	R	R
[Imprimir e excluir o diário do scanner]	R	R/W	R	R	R	R
[Autenticação externa: Definição de substituição do caminho da pasta]	R	R/W	R	R	R	R

[Definições de leitura]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Nível de sensibilidade A.C.S.]	R	R/W	R	R	R	R
[Tempo de espera para próximo(s) original(is)]	R	R/W	R	R	R	R
[Densidade de fundo para ADS (Quatro cores)]	R	R/W	R	R	R	R
[Detectar página em branco]	R	R/W	R	R	R	R

[Definições de envio]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Compactação (Preto e branco)]	R	R/W	R	R	R/W	R
[Compactação (Escala de cinza/Quatro cores)]	R	R/W	R	R	R/W	R
[PDF digitalizado via OCR: Sensibilidade a páginas em branco]	R	R/W	R	R	R/W	R
[Nível de PDF de alta compactação]	R	R/W	R	R	R/W	R
[Método de compactação para PDF de alta compactação]	R	R/W	R	R	R/W	R
[Tamanho máx. de e-mail]	R	R	R/W	R	R*1	R*1
[Dividir e enviar e-mail]	R	R	R/W	R	R*1	R*1
[Inserir informações adicionais de e-mail]	R	R/W	R	R	R/W	R
[N° de dígitos para arquivos de páginas únicas]	R	R/W	R	R	R/W	R
[Método de e-mail em arquivo armazenado]	R	R/W	R	R	R/W	R
[Assunto padrão de e-mail]	R	R/W	R	R	R	R

*1 Quando a opção [Gestão de rede] em [Gestão de autenticação do administrador] é definida como [Desligado], os usuários recebem privilégios R/W (leitura/gravação).

[Definições iniciais]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Proteger menu]	R	R/W	R	R	R	R
[Usar WSD ou DS]	R	R/W	R	R	R	R
[Exibir lista de destinos WSD]	R	R/W	R	R	R	R
[Proibir comando de leitura WSD]	R	R/W	R	R	R	R
[Usar uma lista de destinos que não seja DSM]	R	R/W	R	R	R	R

[Definições padrão para telas normais do dispositivo]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Armazenar arquivo]	–	R/W	–	–	R	R
[Visualização]	–	R/W	–	–	R	R
[Definições de leitura]	–	R/W	–	–	R	R
[Tipo de arquivo de envio]	–	R/W	–	–	R	R

[Definições padrão para telas simplificadas do dispositivo]

Definições	Usuário	Equip	N/W	Arquivo	Nív.1	Nív.2
[Definições de leitura]	–	R/W	–	–	R	R
[Tipo de arquivo de envio]	–	R/W	–	–	R	R

Web Image Monitor: Interface

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

[Definições de interface]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Rede]	R	R	R	R	R	R
[Endereço MAC]	R	R	R	R	R	R
[Segurança da Ethernet]	R	R	R/W	R	R/W	R
[Velocidade da Ethernet]	R	R	R/W	R	R/W	R
[Host USB]	R	R/W	R	R	R/W	R

Web Image Monitor: Rede

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

[IPv4]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[IPv4]	R	R	R/W*1	R	R/W*1	R
[Nome do host]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Nome de domínio]	R	R	R/W	R	R/W	R
[Endereço IPv4]	R	R	R/W	R	R/W	R
[Máscara de sub-rede]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Servidor WINS principal]	R	R	R/W	R	R/W	R
[Servidor WINS secundário]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[ID de escopo]	R	R	R/W	R	R/W	R
[Detalhes]	R	R	R/W	R	R/W	R

*1 Não é possível desativar IPv4 ao usar Web Image Monitor com uma conexão IPv4.

[IPv6]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[IPv6]	R	R	R/W*2	R	R/W*2	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Nome do host]	R	R	R/W	R	R/W	R
[Nome de domínio]	R	R	R/W	R	R/W	R
[Endereço link-local]	R	R	R	R	R	R
[Endereço sem monitoração de estado]	R	R	R/W	R	R/W	R
[Endereço de configuração manual]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[Endereço DHCPv6]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Detalhes]	R	R	R/W	R	R/W	R

*2 Não é possível desativar IPv6 ao usar Web Image Monitor com uma conexão IPv6.

[NetWare]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[NetWare]	R	R	R/W	R	R/W	R
[Definições de impressão NetWare]	R	R	R/W	R	R/W	R
[Entrega NCP]	R	R	R/W	R	R/W	R

[SMB]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[SMB]	R	R	R/W	R	R/W	R
[Protocolo]	R	R	R	R	R	R
[Nome do grupo de trabalho]	R	R	R/W	R	R/W	R
[Nome do computador]	R	R	R/W	R	R/W	R

Definições	Usuár io	Equip	N/W	Arqui vo	Unset	Defini do
[Comentário]	R	R	R/W	R	R/W	R
[Nome do compartilhamento]	R	R	R	R	R	R
[Notificar conclusão da impressão]	R	R	R/W	R	R/W	R

[SNMP]

Definições	Usuár io	Equip	N/W	Arqui vo	Unset	Defini do
[SNMP]	–	–	R/W	–	–	–
[Protocolo]	–	–	R/W	–	–	–
[Definição SNMPv1,v2]	–	–	R/W	–	–	–
[Comunidade]	–	–	R/W	–	–	–

[SNMPv3]

Definições	Usuár io	Equip	N/W	Arqui vo	Unset	Defini do
[SNMP]	–	–	R/W	–	–	–
[Protocolo]	–	–	R/W	–	–	–
[Definição SNMPv3]	–	–	R/W	–	–	–
[Definição de comunicação Trap SNMPv3]	–	–	R/W	–	–	–
[Conta (Usuário)]	–	–	R/W	–	–	–
[Conta (Administrador de rede)]	–	–	R/W	–	–	–
[Conta (Administrador de máquina)]	–	R/W	–	–	–	–

[SSDP]

Definições	Usuár io	Equip	N/W	Arqui vo	Unset	Defini do
[SSDP]	–	–	R/W	–	–	–

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[UUID]	–	–	R	–	–	–
[Perfil expira]	–	–	R/W	–	–	–
[TTL]	–	–	R/W	–	–	–

[Bonjour]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Bonjour]	R	R	R/W	R	R/W	R
[Nome do host local]	R	R	R	R	R	R
[Detalhes]	R	R	R/W	R	R/W	R
[Prioridade de ordem de impressão]	R	R	R/W	R	R/W	R

[Log do sistema]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Log do sistema]	R	R	R	R	R	–

Web Image Monitor: Segurança

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Segurança da rede]	–	–	R/W	–	–	–
[Controle de acesso]	–	–	R/W	–	–	–
[Autenticação IPP]	–	–	R/W	–	–	–
[SSL/TLS]	–	–	R/W	–	–	–
[ssh]	–	–	R/W	–	R	R
[Certificado do site]	–	–	R/W	–	–	–
[Certificado de dispositivo]	–	–	R/W	–	–	–
[S/MIME]	–	–	R/W	–	–	–
[IPsec]	–	–	R/W	–	–	–
[Política de bloqueio do usuário]	–	R/W	–	–	–	–
[IEEE 802. 1X]	–	–	R/W	–	–	–
[Extended Security]						
• [Chave de criptografia de driver]	–	–	R/W	–	R/W	–
• [Driver Encryption Key: Encryption Strength]	R	R	R/W	R	R/W	R
• [Restringir visualiz de info de usuários]	R	R/W	R	R	R/W	R
• [Encrypt User Custom Settings & Address Book]	R/W	R	R	R	R	R
• [Enhance File Protection]	R	R	R	R/W	R	R
• [Restrict Use of Destinations (Scanner)]	R/W	R	R	R	R	R
• [Restringir adição de destinos de usuários (Scanner)]	R/W	R	R	R	R	R
• [Authenticate Current Job]	R	R/W	R	R	R/W	R

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
• [@Remote Service]	R	R/W	R	R	R/W	R
• [Update Firmware]	R	R/W	R	R	–	–
• [Change Firmware Structure]	R	R/W	R	R	–	–
• [Password Policy]	R/W	–	–	–	–	–
• [Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
• [Security Setting for Access Violation]	–	R/W	–	–	–	–
• [Violação de entrada de senha]	–	R/W	–	–	–	–
• [Violação de acesso do dispositivo]	–	R/W	–	–	–	–

Web Image Monitor: @Remote

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Configurar RC Gate]	–	R/W	–	–	–	–
[Atualizar firmware do RC Gate]	–	R/W	–	–	–	–
[Servidor proxy do RC Gate]	–	R/W	–	–	–	–
[Notificar problemas funcionais do dispositivo]	–	R/W	–	–	–	–

Web Image Monitor: Página Web

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

[Página da Web]

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Idioma da página da Web]	R	R	R/W	R	R/W	R
[Logout automático do Web Image Monitor]	R	R	R/W	R	R/W	R
[Definir alvo da URL da Ajuda]	R	R	R/W	R	R/W	R
[Definir alvo da URL da Ajuda]	R	R	R/W	R	R/W	R
[Definição de WSD/UPnP]	R	R	R/W	R	R/W	R
[Fazer download do arquivo de ajuda]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: Definições de funções avançadas

Essas definições estão em [Configuração] em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Definição de inicialização]	–	R/W	–	–	–	–
[Informações sobre recurso estendido]	R	R	R	R	R	R
[Instalar]	–	R/W	–	–	–	–
[Desinstalar]	–	R/W	–	–	–	–
[Ferramentas de administrador]	–	R/W	–	–	–	–
[Definição de inicialização de programa adicional]	–	R/W	–	–	–	–
[Instalar programa adicional]	–	R/W	–	–	–	–
[Desinstalar programa adicional]	–	R/W	–	–	–	–
[Copiar recursos estendidos]	–	R/W	–	–	–	–
[Copiar dados salvos do cartão]	–	R/W	–	–	–	–

Web Image Monitor: Livro de endereços

Estas definições estão em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Adicionar usuário]	R/W	–	–	–	R/W *1	R/W *1
[Alterar]	R/W	–	–	–	R/W *1	R/W *1
[Excluir]	R/W	–	–	–	R/W *1	R/W *1
[Adicionar grupo]	R/W	–	–	–	R/W *1	R/W *1
[Definição de transporte de dados para o programa automático do catálogo de endereços]	R/W	–	–	–	R/W	R
[Manutenção]	R/W	–	–	–	–	–
[Gerenciamento central do Catálogo de endereços]	R/W	–	–	–	–	–

*1 Se [Restringir adição de destinos de usuários] de [Segurança estendida] for definido como [Ligado] e a autenticação básica for aplicada ao equipamento, cada usuário só poderá alterar a senha para a sua conta.

Web Image Monitor: Gerenciamento central do Catálogo de endereços

Estas definições estão em [Gerenciamento do dispositivo].

Essa definição não aparecerá se você tiver privilégio de administrador de usuários. Nesse caso, especifique acessando [Gerenciamento do dispositivo] > [Catálogo de endereços].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Gerenciamento central do Catálogo de endereços]	–	R/W	–	–	–	–

Web Image Monitor: Desligado

Estas definições estão em [Gerenciamento do dispositivo].

Definições	Usuári o	Equip	N/W	Arqui vo	Unset	Defini do
[Modo desligado]	–	R/W	–	–	–	–
[OK]	–	R/W	–	–	–	–

Web Image Monitor: Apagar trabalho de impressão

Estas definições estão em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Redefinir trabalho atual]	–	R/W	–	–	–	–
[Redefinir todos os trabalhos]	–	R/W	–	–	–	–

Web Image Monitor: Reiniciar o equipamento

Estas definições estão em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

Definições	Usuári o	Equip	N/W	Arqui vo	Unset	Defini do
[Redefinir a máquina]	–	R/W	–	–	R/W	–

Web Image Monitor: Redefinir a máquina

Estas definições estão em [Gerenciamento do dispositivo].

Quando é definida a autenticação do administrador, as restrições às operações dos usuários diferem dependendo da configuração em "Definições disponíveis".

Definições	Usuári o	Equip	N/W	Arqui vo	Unset	Defini do
[Editar ícones]	R	R/W	R	R	R/W	R
[Restaurar exibição padrão de ícones]	–	R/W	–	–	R/W	–
[Definições da tela inicial]	R	R/W	R	R	R/W	R

Web Image Monitor: Monitoramento de tela

Estas definições estão em [Gerenciamento do dispositivo].

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Exibir tela do dispositivo]	–	R/W	–	–	–	–

9

Web Image Monitor: Personalizar tela por usuário

Esta informação aparecerá se a opção [Personalização do usuário] estiver definida como [Permitir].

Os usuários poderão alterar apenas suas próprias definições.

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Editar ícones]	–	–	–	–	–	R/W
[Restaurar exibição padrão de ícones]	–	–	–	–	–	R/W
[Prioridade da função por usuário]	–	–	–	–	–	R/W

Web Image Monitor: Servidor de documentos

Estas definições estão em [Imprimir trabalho/arquivo armazenado].

O que os usuários podem fazer com arquivos armazenados depende de seus privilégios de acesso. Para mais informações, consulte Pág. 359 "Lista de privilégios de operações em arquivos armazenados".

Definições	Usuári o	Equip	N/W	Arqui vo	Unset	Defini do
[Nova pasta]	–	–	–	R/W	R/W	R/W
[Editar pasta]	–	–	–	R/W	R/W	R/W
[Excluir pasta]	–	–	–	R/W	R/W	R/W
[Desbloquear pasta]	–	–	–	R/W	–	–
[Imprimir]	–	–	–	–	R/W	R/W
[Enviar]	–	–	–	–	R/W	R/W
[Excluir]	–	–	–	R/W	R/W	R/W
[Editar informações detalhadas]	–	–	–	R/W	R/W	R/W
[Download]	–	–	–	–	R/W	R/W
[Desbloquear arquivo]	–	–	–	R/W	–	–

9

Web Image Monitor: Impressora: Imprimir trabalhos

Estas definições estão em [Imprimir trabalho/arquivo armazenado].

Os documentos da impressora que os usuários podem gerenciar são os que foram armazenados por eles próprios ou quando a autenticação de usuário está desativada.

Os documentos de impressão armazenados por outros usuários não são mostrados.

Definições	Usuário	Equip	N/W	Arquivo	Unset	Definido
[Imprimir]	–	–	–	–	R/W*1	R/W*1
[Excluir]	–	–	–	R/W	R/W*1	R/W*1
[Editar informações detalhadas]	–	–	–	R/W	R/W*1	R/W*1
[Desbloquear trabalho]	–	–	–	R/W	–	–

*1 O acesso aos documentos salvos pode ser restrito, dependendo dos privilégios de acesso do usuário.

9

Lista de privilégios de operações em arquivos armazenados

Significado dos tipos cabeçalhos

- Ler

  Usuários com privilégios de leitura.

- Editar

  Usuários com privilégios de edição.

- E/D

  Usuários com privilégios de edição/exclusão.

- Total

  Usuários com privilégios de controle total.

- Proprietário

  Indica o usuário que registrou o documento ou um usuário especificado como proprietário.

- Arquivo

  Indica o administrador de arquivos.

Significado dos símbolos

R/W: Permissão para execução

–: Sem permissão para execução

Definições	Ler	Editar	E/D	Total	Propriet ário	Arquivo
[Imprimindo]	R/W	R/W	R/W	R/W	R/W	–
[Detalhes]	R/W	R/W	R/W	R/W	R/W	R/W
[Visualização]	R/W	R/W	R/W	R/W	R/W	–
[Alt. priv. de acesso]: [Proprietário]	–	–	–	–	–	R/W
[Alt. priv. de acesso]: [Permissões para usuários/grupos]	–	–	–	R/W	R/W*1	R/W
[Alterar nome do arquivo]	–	R/W	R/W	R/W	R/W*1	–
[Alterar senha]	–	–	–	–	R/W	R/W
[Desbloq. arquivos]	–	–	–	–	–	R/W

Definições	Ler	Editar	E/D	Total	Proprietário	Arquivo
[Combinar arquivos]	–	–	R/W	R/W	R/W*1	–
[Inserir arquivo]	–	–	R/W	R/W	R/W*1	–
[Excluir páginas]	–	–	R/W	R/W	R/W*1	–
[Duplicar arquivo]	R/W	R/W	R/W	R/W	R/W*1	–
[Excluir arquivo]	–	–	R/W	R/W	R/W*1	R/W
[Impr. pág. espec]	R/W	R/W	R/W	R/W	R/W*1	–
[Manter defs de 2 /1 lado]	R/W	R/W	R/W	R/W	R/W*1	–

*1 O proprietário pode alterar privilégios de operação.

[Combinar arquivos] e [Inserir arquivo] pode ser aplicado aos arquivos com a permissão de acesso "Editar/Excluir".

Ao executar [Combinar arquivos] ou [Inserir arquivo], a permissão de acesso configurada para o arquivo selecionado inicialmente é aplicada no arquivo recentemente criado.

Lista de privilégios de operações para Catálogos de endereços

Significado dos tipos cabeçalhos

- Ler

  Usuários com privilégios de leitura.

- Editar

  Usuários com privilégios de edição.

- E/D

  Usuários com privilégios de edição/exclusão.

- Total

  Usuários com privilégios de controle total.

- Entrada

  Indica um usuário cujas informações pessoais estejam registradas no Catálogo de endereços. Também indica qualquer usuário que conheça seu nome e senha de login de usuário.

- Usuário

  Indica o administrador do usuário.

Significado dos símbolos

R/W: Permissão para execução, alteração e leitura.

R: Permissão para leitura.

–: Sem permissão para execução, alteração e leitura.

[Nomes]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[Nome]	R	R/W	R/W	R/W	R/W	R/W
[Exibição da tecla]	R	R/W	R/W	R/W	R/W	R/W
[N° de registro]	R	R/W	R/W	R/W	R/W	R/W
[Prioridade de exibição]	R	R/W	R/W	R/W	R/W	R/W
[Selecionar título]	R	R/W	R/W	R/W	R/W	R/W

[Inform Aut.]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[Código do usuário]	–	–	–	–	–	R/W
[Nome de usuário de login]	–	–	–	–	R	R/W
[Senha de login]	–	–	–	–	R/W*1	R/W*1
[Autenticação SMTP]	–	–	–	–	R/W*1	R/W*1
[Autenticação de pasta]	R	R/W*1	R/W*1	R/W*1	R/W*1	R/W*1
[Autenticação de LDAP]	–	–	–	–	R/W*1	R/W*1
[Funções disponíveis]	–	–	–	–	R	R/W
[Vol imp Limit de uso.]	–	–	–	–	R	R/W

*1 Senhas não podem ser lidas.

[Proteção]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[Usar nome como]	R	R/W	R/W	R/W	R/W	R/W
[Proteger destino]: [Código de proteção]	–	–	–	R/W*2	R/W*2	R/W*2
[Proteger destino]: [Objeto de proteção]	–	R/W	R/W	R/W	R/W	R/W
[Proteger destino]: [Permissões para usuários/grupos]	–	–	–	R/W	R/W	R/W
[Proteger arquivo(s)]: [Permissões para usuários/grupos]	–	–	–	R/W	R/W	R/W

*2 O código para [Código de proteção] não pode ser lido.

[E-mail]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[Endereço de e-mail]	R	R/W	R/W	R/W	R/W	R/W

[Pasta]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[SMB/FTP/NCP]	R	R/W	R/W	R/W	R/W	R/W
[SMB]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Nome do servidor]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [Número da porta]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Caminho]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [Tipo de conexão]	R	R/W	R/W	R/W	R/W	R/W
[Teste de conex]	R	R/W	R/W	R/W	R/W	R/W

[Adic. ao grupo]

Definições	Ler	Editar	E/D	Total	Entrada	Usuário
[N° de registro]	R	R/W	R/W	R/W	R/W	R/W
[Pesquisar]	R	R/W	R/W	R/W	R/W	R/W
[Trocar título]	R/W	R/W	R/W	R/W	R/W	R/W

- Quando [Restringir adição de destinos de usuários] de [Segurança estendida] estiver definido como [Ligado], independentemente dos privilégios, só o administrador de usuários poderá acessar o Catálogo de endereços.

ÍNDICE

R

S

U

V